2002-09

The evolution and application of technical risk management within the United States Navy

Wheeler, Michael A.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

THE EVOLUTION AND APPLICATION OF TECHNICAL RISK MANAGEMENT WITHIN THE UNITED STATES NAVY

by

Michael A. Wheeler

September 2002

Principal Advisor: Ramish Kolar
Associate Advisor: Mike McCune

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: The Evolution and Application of Technical Risk Management within the United States Navy			**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael A. Wheeler			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

This research examines how technical risk management has evolved throughout the Department of the Navy (DoN) and to what extent acquisition programs have implemented best practice methods and techniques. A sample of DoN program managers, risk managers, and other acquisition professionals was surveyed to determine attitudes on technical risk management and what fundamental methods are being applied. Survey data was also collected to determine what impact Department of Defense (DoD) and DoN technical risk guidance has had on the acquisition community and what guidance documents are being used. For cases where best-in-class technical risk management methods and techniques have not been applied, this research offers some potential solutions.

14. SUBJECT TERMS Technical Risk Management, Risk Management, Risk Assessment, Risk Analysis, Probabilistic Risk Assessment, Best Practices, Systems Engineering, Engineering Discipline, Process Rigor.			**15. NUMBER OF PAGES** 174
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

THE EVOLUTION AND APPLICATION OF TECHNICAL RISK MANAGEMENT WITHIN THE UNITED STATES NAVY

Michael A. Wheeler
ND-0830-IV, NSWC Corona Division, United States Navy
B.S., University of Vermont, 1986

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN PRODUCT DEVELOPMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2002

Author: Michael A. Wheeler

Approved by: Ramesh Kolar, Principal Advisor

Mike McCune, NSWC Corona, Associate Advisor

Phil E. DePoy
Director, Wayne E. Meyer Institute of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research examines how technical risk management has evolved throughout the Department of the Navy (DoN) and to what extent acquisition programs have implemented best practice methods and techniques. A sample of DoN program managers, risk managers, and other acquisition professionals was surveyed to determine attitudes on technical risk management and what fundamental methods are being applied. Survey data was also collected to determine what impact Department of Defense (DoD) and DoN technical risk guidance has had on the acquisition community and what guidance documents are being used. For cases where best-in-class technical risk management methods and techniques have not been applied, this research offers some potential solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

APM	Acquisition Program Manager
ASN(RD&A)ABM	Office of the Assistant Secretary of the Navy, Research Development & Acquisition, Acquisition and Business Management
BMPCOE	Best Manufacturing Practices Center of Excellence
C(f)	Consequence of Occurrence
CDR	Critical Design Review
CINC	Commander In Chief
CJCS	Chairman of the Joint Chiefs of Staff
CMM	Capability Maturity Model
COTS	Commercial-Off-The-Shelf
CPM	Critical Path Method
CPU	Central Processing Unit
DAB	Defense Acquisition Board
DAU	Defense Acquisition University
DAWIA	Defense Acquisition Workforce Improvement Act
DMSMS	Diminishing Manufacturing Sources & Material Shortages
DoD	Department of Defense
DoN	Department of the Navy
DSB	Defense Science Board
DSMC	Defense Systems Management College
EAC	Estimate At Completion
EMD	Engineering & Manufacturing Development
FAR	Federal Acquisition Regulation
FMEA	Failure Modes Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
IBR	Integrated Baseline Review
IOC	Initial Operating Capability
IMS	Integrated Master Schedule
I/O	Input/Output
IPPD	Integrated Product & Process Development
IPT	Integrated Product Team
KPA	Key Process Area
MOE	Measures of Effectiveness
MS	Milestone
NASA	National Aeronautics and Space Administration
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NDI	Non-Developmental Item
OO	Object Oriented
OPEVAL	Operational Evaluation

P(f)	Probability of Occurrence
P-CMM	People Capability Maturity Model
PDR	Preliminary Design Review
PEO	Program Executive Officer
PEO TSC	Program Executive Officer Theater Surface Combatants
PM	Program Manager
PMWS	Program Manager's Workstation
POA&M	Plan of Action and Milestones
PQM	Production, Quality and Manufacturing
PRA	Probabilistic Risk Assessment
PRR	Production Readiness Review
R&D	Research and Development
RE	Risk Exposure
RMC	Risk Management Coordinator
RO	Risk Officer
SA-CMM	Software Acquisition Capability Maturity Model
SECNAV	Secretary of the Navy
SEI	Software Engineering Institute
SEMT	Systems Engineering Management Team
SFR	Systems Functional Review
SOO	Statement of Objectives
SPAWAR	Space and Naval Warfare Systems Command
SPRDE	Systems Planning, Research, Development, and Engineering
SRR	Systems Requirements Review
SVR	Systems Verification Review
SW-CMM	Software Capability Maturity Model
TDA	Technical Direction Agent
TPM	Technical Performance Measure
TRIMS	Technical Risk Identification and Mitigation System
WBS	Work Breakdown Structure
WSESRB	Weapon System Explosive Safety Review Board

ACKNOWLEDGMENTS

I would like to thank my family for their love, support, and patience over the past two years. I dedicate this work to each and every one of them. Without their support I could never have done this. A special thanks to my wife, Veronica, for always being there for me, encouraging me along the way, and loving me unconditionally.

Thanks to my Mom and Dad for teaching me the value of education and instilling in me the discipline to succeed. Thanks to my precious children, Brandon, Justin, and baby Joshua for giving up their daddy many nights to the dreaded "homework monster." Thanks to Dorothy and John for helping with the family, so I could pursue my dream. Thanks to the leadership at NSWC Corona for allowing me this opportunity pursue a masters program and for their support all along this journey. Thanks to my colleagues, peers, and co-workers for their patience with my many questions and assistance with my research. Thanks to my thesis advisors for their guidance and many hours of proofing my work.

A special thanks to Mr. Mike McCune, my mentor, who has guided me along my career path since I was a young pup fresh out of college. Your advice has been truly appreciated. I will always be thankful.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Technical risk management is the assessment and management of risk related to the lack of critical engineering disciplines during the design, development, and production of a system. Technical risk is the driver behind all other risk including cost and schedule risk. In 1985, the Defense Science Board claimed that once rigorous and disciplined engineering practices were employed and institutionalized, the risk of deploying unsuitable weapon systems would be low and the time in the acquisition cycle would be reduced (DoD 4245.7-M, 1985, p. 1). This is still true today with the focus on the systems engineering process as the means to ensure key engineering disciplines have been implemented. Technical risk management methods and techniques measure how well engineering disciplines have been applied and provide an early warning to potentially costly problems from surfacing later in the acquisition cycle.

A 1997 survey of 41 Navy program offices by ASN(RD&A)ABM revealed no common or consistent methodology for technical risk management. As a result, ASN(RD&A)ABM released a guidance document (NAVSO P-3686) for program managers in October 1998 containing technical risk management best practices. The document was entitled, *Top Eleven Ways to Manage Technical Risk*. After nearly four years, a review of this document's impact on the Navy acquisition community was studied in this thesis.

A sample of Department of the Navy (DoN) program managers, risk managers, and other acquisition professionals was surveyed to determine attitudes on technical risk management and what fundamental methods are being applied. Survey data was also collected to determine what impact Department of Defense (DoD) and DoN technical risk guidance has had on the acquisition community and what guidance documents are being used. For cases where best-in-class technical risk management methods and techniques have not been applied, this research offers some potential solutions.

This research obtained the following results and conclusions:

- There has been a tremendous evolution of technical risk management methods and techniques within DoN over the course of nearly 20 years driven by acquisition reform.
- Although risk management and assessment is clearly part of a program manger's tool kit today, technical risk management methods and techniques have not been institutionalized throughout the Navy.
- There is need for more technical risk management training throughout the Navy acquisition community. 20% of those surveyed have not received risk training.
- Technical risk management is very important to the success of an acquisition program.
- Qualitative technical risk management methods are predominately used within the Navy.
- There is a definite correlation between systems engineering and technical risk management.
- Incentives for applying technical risk management methods and techniques are lacking.
- Unmitigated Process risk leads to Product risk.
- A risk awareness or risk friendly culture where program risks are openly discussed has not been fully institutionalized within the Navy.
- Nearly one-third of those surveyed don't apply software risk management methods.
- 36% of those surveyed have used or are using NAVSO P-3686. 44% have used or are using DoD 4245.7-M (Willoughby Templates), NAVSO P-6071 (Best Practices), or *Methods & Metrics for Product Success* as guidance for their technical risk management programs.
- Approximately 70% of those surveyed did not know what technical risk guidance documents their contractor's were using. 30% used the same guidance documents as their contractors.
- Nearly 20% of those surveyed believe DoD, SECNAV, and NAVSEA risk management policy was inadequate. Another 40% were neutral on this issue.
- Nearly 20% of those surveyed were dissatisfied with their risk management programs and another 40% were neutral.

Although the Navy has made strides over the course of 20 years with technical risk management awareness and need, there are still weaknesses in the application and implementation of proactive technical risk management methods and the open communication of risk within the Navy acquisition community.

I. INTRODUCTION

A. ACQUISITION REFORM – A CULTURAL CHANGE

1994 marked a significant cultural change in the way the Department of Defense (DoD) does business. Three major events occurred which mandated this change. In February, Secretary of Defense Dr. William Perry issued a mandate for change (DSMC, 2002a, ¶ 3) in a paper to all defense departments and agencies entitled, *Acquisition Reform: A Mandate for Change*. This paper provided a conceptual look at DoD's approach to acquisition reform. Defenselink's Web Site states, "DoD will institutionalize business processes that facilitate affordable and timely delivery of best-value products and services that meet warfighter needs." (Defenselink, 2002a, ¶ 3). In June, Secretary Perry issued a memorandum to all defense departments and agencies directing the replacement of all military standards and specifications with commercial specifications (Perry, 1994). Use of military specifications and standards were authorized only as a last resort and if a waiver was granted. Finally, in October, the Federal Acquisition Streamlining Act was signed into law, which overhauled the bureaucratic, complex, and cumbersome procurement process within the federal government (DSMC, 2002b, ¶ 1). The Act mandated that DoD, "increase the use of commercially available items where practicable, place more emphasis on past contractor performance, and promote best value rather than simply low cost in selecting sources of supplies and services." (Powell, J. E., 2002, p. 65).

With these defining events acquisition reform was born. Defense Systems Management College (DSMC), now known as Defense Acquisition University (DAU), defines this cultural change as:

> Acquisition reform, a theory pervasive throughout the Department of Defense, is an endeavor to make the acquisition process more effective, efficient, and productive. It involves reducing overhead, streamlining requirements, speeding up processes, cutting paperwork and other similar initiatives to reduce bureaucracy. Acquisition reform includes a move toward the use of commercial practices as well as the use of private enterprise to do more of the functions traditionally done by government. (DSMC, 2002c, ¶ 1)

On 10 May 1995, Secretary Perry issued a memorandum to the Service Secretaries mandating the use of Integrated Product Teams (IPT) throughout the acquisition process ("Why Do We Need IPTs?", 2002, ¶ 1). This decision was based on Boeing's success with Integrated Product & Process Development (IPPD) on the 777 Program (Schaeffer, 1997, p. 51). This author believes this IPT mandate has been one of the few quantifiable successes of acquisition reform. In his memo Secretary Perry defined IPPD as, "A management process that integrates all activities from product concept through production/field support, using a multi-functional team, to simultaneously optimize the product and its manufacturing and sustainment processes to meet cost and performance objectives." ("IPPD definitions," 1995, ¶ 2) The memo lists 10 key tenets of IPPD with number 10 being "Proactive Identification and Management of Risk." This effectively makes risk analysis and management a key responsibility of IPTs. It requires critical cost, schedule, and performance parameters to be identified by IPTs using a risk analysis (assessment) process. It also requires that performance measures (i.e., metrics) be identified and compared to industry benchmarks and best practices for cost, schedule, and performance control and achievement of technical and business parameters. ("IPPD definitions," 1995, ¶ 2) This best practice and lessons learned approach to technical risk management is precisely the approach followed by many within the Navy and will be described in subsequent chapters. Measuring the variance between a program's practice and a government or industry best practice is an effective technical risk management approach which mitigates process related risk early before it is manifested in the product (hardware/software).

Reig (Reig, 2000, pp. 33-36) provides an excellent summary of acquisition reform events. Table 1 provides a chronology of significant acquisition reform events in the 1990s. Table 2 provides an alphabetical list of acquisition reform initiatives.

Table 1. Chronology of Acquisition Reform Events. From (Reig, 2000, pp. 35-36)

Date	Event
February 1991	DoDD 5000.1 DoDI 5000.2 changed and reissued and 5000.2M promulgated.
January 1993	The Acquisition Law Advisory Panel (Section 800 Panel) findings reported to Congress.[a]
June 1993	Colleen Preston assumes the position as Deputy Under Secretary of Defense for Acquisition Reform.[a]
October 1993	Federal Acquisition Streamlining Act (FASA) of 1994 enacted.[a]
First quarter 1994	The Advanced Concept Technology Demonstration program initiated.[b]
February 1994	William J. Perry replaces Les Aspin as Secretary of Defense.[a]
February 1994	Secretary Perry issues "Acquisition Reform, A Mandate for Change."[a]
March 1994	Secretary Perry attaches "Mandate for Change" to a letter to the leadership of the Department of Defense.[a]
June 1994	Preston authors an article, "Acquisition Reform—Making it a Reality," in *Phalanx: the Bulletin of Military Operations Research* (June 1994, 27[2]). The article concludes with a section titled, "How Can You Participate?"[a]
June 1994	Secretary Perry issues memo: "Specifications and Standards—A New Way of Doing Business."[a]
October 1994	Paul Kaminski sworn in as Under Secretary of Defense for Acquisition and Technology (USD[A&T]).[a]
c. 1994	DUSD(AR) position to report to USD(A&T).[a]
December 1994	The Oversight and Review of the Systems Acquisition Process PAT report published.[b]
December 1994	The Defense Acquisition Pilot Program launched as allowed by FASA.
March 1995	USD(A&T) establishes an IPT for the purpose of rewriting the February 23, 1991, 5000 Series documents.[b]
April 1995	Kaminski issues a memorandum, "Reengineering the Acquisition Oversight and Review Process." First recommendations of the PAT team approved.[b]

(continued)

Table 1. Chronology of Acquisition Reform Events. From (Reig, 2000, pp. 35-36) (continued)

Date	Event
May 1995	Secretary Perry implements the IPT concept for DoD via a memorandum.[a]
July 1995	Kaminski holds a DoD offsite entitled "Institutionalizing IPTs—DoD's Commitment to Change."[b]
November 1995	Rules of the Road: A Guide for Leading Successful Integrated Product Teams is published.[b]
December 1995	CAIV was initiated.[a]
December 1995	USD(A&T) issues guidance for making "class action" contract changes to existing contracts on a facility-wide basis. AKA Single Process Initiative (SPI).[b]
February 1996	*DoD Guide to Integrated Product and Process Development*, (Version 1.0) issued by the OUSD(A&T).[a]
February 1996	Director, Test, Systems Engineering, and Evaluation, publishes DoD Guide to IPPD, Version 1.0.[b]
March 1996	Update of the DoD 5000 Documents approved by the USD(A&T), DOT&E, and ASD (C3I).[a]
March 1996	The ODUSD(AR) produces the video The Overarching and Working Level Integrated Product Teams, and the OIPT-WIPT Information Guide.[b]
April 1996	DoD and Texas Instruments sign first SPI agreement for manufacturing standards for all its products.[b]
May 1996	DoD Acquisition Reform Day is held.[b]
July 1996	The *Defense Acquisition Deskbook*, first piece, released.[b]
September 1996	Kaminski's memorandum provides guidance for dealing with specification or process changes on subcontracts (SPI).[b]
December 1996	The publishing of DoD 5000.2R, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs.* (Includes change 1).[a]

[a] All data and information obtained from Defense Systems Management College. (1997, December). A Model for Leading Change: Making Acquisition Reform Work (report of the 1996-1997 DSMC Military Research Fellows). Fort Belvoir, VA: Author.

[b] All data and information obtained from Defense Systems Management College. (1997, January-February). Acquisition reform —the end of the beginning. *Program Manager* (special issue), 26(1).

Table 2. Acquisition Reform Initiatives. From (Reig, 2000, p. 37)

Acquisition Law Advisory Panel (Section 800 Panel)
Audit/Inspection Reform
Advanced Concept Technology Demonstration (ACTD)
Buying Commercial
Defense Acquisition Deskbook
Defense Acquisition Pilot Programs (DAPP)
Direct Vendor Delivery
Dual-Use Technology
Electronic Commerce
Empowerment
Federal Acquisition Streamlining Act of 1994 (FASA)
Integrated Product and Process Teams
Lean Logistics
Modeling and Simulation
Multiyear Contracts
Outsourcing
Partnerships with Industry
Performance-Based Contracting
Privatization
Program Stability
Reduced Government Oversight
Reengineering the Acquisition Oversight and Review Process
Single Process Initiative (SPI)
Specifications and Standards Policy
Streamlined Solicitation Packages
Update and Reissue of the DoD 5000 Series Documents
Workforce Education

There is one significant event missing from Reig's chronology which is worthy of mention because it had a significant impact on acquisition reform and operational and technical authority within DoD. The 1986 Goldwater-Nichols Department of Defense Reorganization Act had a profound impact on the DoD requirements generation system and the players involved in establishing the mission need and advancing warfighting requirements. It also significantly altered the responsibility for acquisition oversight.

Goldwater-Nichols centralized operational authority through the Chairman of the Joint Chiefs (CJCS) (NDUL, 2002, ¶ 1). CJCS acts as a spokesman for the Commander In Chiefs (CINC) integrating and prioritizing their requirements. Prior to this Act, the Service Chiefs defined their own requirements, and they often were more concerned with maintaining and promoting their own interests. (Osgood, 1996, ¶ 5) Goldwater-Nichols put in place a joint operational approach under the exclusive command of the CINC on the battlefield. It instilled a joint service approach to requirements generation eliminating often duplicative approaches from the Services. The Services went from defining requirements and leading operations prior to Goldwater-Nichols to providing capabilities to the CINCs (Goldwater-Nichols," n.d., p. 14).

Goldwater-Nichols also created a civilian controlled acquisition function moving the responsibility for oversight from the military to a civilian acquisition executive under each Service Secretary. This legislature empowered program managers to be the single authority for their acquisition programs reporting to the civilian acquisition executive. Within the Department of the Navy (DoN) acquisition Program Managers (PM) and Program Executive Officers (PEO) report directly to Office of Assistant Secretary of the Navy, Research, Development and Acquisition ASN(RD&A). The objective was to streamline the acquisition organization, processes, and communication within the acquisition community. What it did instead was to divest the program managers from a technical authority framework within the Services. This technical authority provided checks and balances on the implementation of critical engineering disciplines. Goldwater-Nichols removed these checks and balances and left it up to the PMs to decide what was best for their programs. Often, PMs chose not to implement key disciplines

and practices because of budget constraints, lack of knowledge, or schedule issues. They knowingly and sometimes unknowingly took risks by failing to implement key disciplines. It's ironic that their failure to implement key disciplines and engineering practices actually result in program risk. Prior to Goldwater-Nichols, Headquarters Commands maintained staffs of technical experts responsible for providing technical oversight of acquisition programs. After this Act became law, these commands lost much of their technical talent to downsizing actions and delegation to field activities.

Today, the technical expertise resides at the field activities. However, it remains at the discretion of the PEOs/PMs whether their technical experts within the field activities are consulted. Since the Warfare Centers and Laboratories are Working Capital Fund activities, there is a competitive push for PEO/PM business. Often PEOs/PMs task field activities most familiar to them and not necessarily the subject matter experts. This is an issue within the Naval Sea Systems Command (NAVSEA) because there are no formal and consistent engineering and technical authority assignments. Current NAVSEA policy leaves it up to the PEOs/PMs to make engineering agent assignments for their particular programs. They often choose those field activities most familiar to them, and they may not necessarily task the leading technical authority in a particular area of interest.

Goldwater-Nichols had as much impact on technical risk management as the acquisition reform initiatives already discussed. It is interesting that the literature on acquisition reform rarely discusses this linkage. Divesting the technical authority and oversight for acquisition systems from the military to a separately reporting civilian reporting chain, resulted in significant impacts on warfighting readiness. However, Goldwater-Nichols did not act alone. Acquisition reform allowed the PEOs/PMs to pick and choose the engineering disciplines they applied to their programs. Often they waived key processes and disciplines, which resulted in technical risk. Because today's decisions affect tomorrow's product, the risk often was manifested in hardware and software products later in the acquisition timeline.

Acquisition reform also brought with it a cultural change on how DoD and DoN viewed risk. Traditional risk avoidance techniques were replaced with risk management

methods. Program/project managers and other acquisition personnel had to think about potential program risks and manage their impact on acquisition programs. Risk management was now a key component of program/project management and required due consideration and planning throughout the acquisition life-cycle. Resources for risk mitigation had to be planned for and loaded into the program/project schedules. Dr. Paul Kaminski, former Under Secretary of Defense for Acquisition and Technology, was a firm believer that a cultural change was necessary for reform and it also necessitated a change in how we viewed risk. Dr. Kaminski states,

> …it has become obvious to me that we will need to transform the risk averse culture that has grown up within the department over the years. I can not direct this cultural change—we need 'buy in' by all of you, the major stakeholders. Unless this occurs, we will not develop the trust 'n' teamwork that it takes to implement the Integrated Product Team (IPT) concept. The department's top leadership must create a climate for reasoned risk-taking—otherwise we will never exploit the opportunities that may be within reach. (DSMC, 2002d, ¶ 4)

Dr. Kaminski eloquently characterizes transforming the risk culture resulting from acquisition reform initiatives. He also discusses the importance of gaining buy-in from the acquisition community. He recognized that cultural change is difficult and requires acceptance by all those involved. Unless this buy-in occurs, IPTs would not be focused and aligned toward common goals including promulgating acquisition reform initiatives and identifying and mitigating risk.

Finally, Dr. Kaminski discusses the role of top leadership in this cultural change. With any cultural change of this magnitude top leadership must support the change by creating a working environment conducive to the change. Dr. Kaminski says top leadership must allow managed risk taking. Risk taking is necessary in order to take advantage of opportunity. Top leaders must not punish those who identify risk, i.e., "shoot the messenger approach." There is risk in every program, therefore leadership must accept this fact and carry on with a sound risk management approach to reduce the risk to acceptable levels. The key lies in identifying risk, so it can be managed. The Risk

vs. Opportunities approach is a fundamental aspect of technical risk management within the Navy today and a direct result of acquisition reform.

Nearly 10 years later, there are still those entrenched in senior leadership positions who don't want to hear bad news. They chastise those who bring high risks to the table creating an atmosphere of distrust and adversarial relationships. Opportunities cannot be realized without risk taking. The key is managing the risk, so it does not adversely impact cost, schedule, and performance parameters. An atmosphere of managed risk taking should be encouraged by Navy leadership. PMs must know that they will not be punished for reporting High risks up the chain. A risk awareness culture must permeate all levels of the acquisition community. One of the Technical Risk Management Survey questions contained in this research addresses this cultural issue. If risks are known, they can then be tracked, managed, and reduced to acceptable levels. This author believes the Navy has not completely deployed a risk awareness culture, and it is the direct result of poor support from top Navy leadership. The results of the survey support this contention. Dr. Kaminski was right on the mark when he spoke about this transformation nearly 10 years ago.

B. THE ORIGIN OF STANDARDS & SPECIFICATIONS

Some believe about 3000 years ago the Egyptians established a standard for the unit of length. It was called the Royal Egyptian Cubit. The Royal Cubit Master was carved from a block of granite to last forever. Its length was equal to the length of the forearm from the bent elbow to the tip of the extended middle finger plus the width of the palm of the hand of the Pharaoh ruling at the time. The workers building the pyramids, tombs, and temples were supplied with cubit sticks made from wood or granite equal to the length of the Royal Cubit Master. The Royal Architect or foreman of each construction site was responsible for ensuring that the workers cubit sticks matched the length of and was traceable to the master. This comparison was required at each full moon and failure to do so was punishable by death. The story of the Royal Cubit Master is depicted in the Egyptian papyrus shown in Figure 1. (NCSL, 2002, Papyrus story)

Although this punishment was severe the ancient Egyptians knew the value of standards and traceability. Standardization helped the Egyptians achieve great accuracy. "The Great Pyramid of Giza was constructed to stand roughly a 756 feet or 9,069.4 inches. Using cubit sticks, the builders were within 4.5 inches – an accuracy of 0.05%." (NCSL, 2002, Papyrus story).

Figure 1. The Royal Egyptian Cubit Papyrus. From (NCSL, 2002, Papyrus story)

It is apparent that the ancient Egyptians were firm believers of managing risk through avoidance. They did this by the establishing a set of standards and practices to live by that had to be followed without question or suffer severe consequences.

The ancient Romans were also advocates of standardization and developed many military standards and specifications. One in particular has pervaded our modern culture.

The U.S. standard railroad gauge, which is defined as the distance between the rails, is 4 feet 8.5 inches. This is an odd size, which begs the question, why? The answer lies in our historical ties to England and their past ties to the Roman Empire. English expatriates built the U.S. railroads and that was the gauge they used in England. The first railroads in England were built by the same people who built the tramways. Tramways

pre-dated the railway system in England and that was the gauge they used. Those who built the tramways used the same fixtures and tooling that was used to build wagons, so wagons were built with a wheel spacing of the same gauge. This odd wheel spacing was used because it exactly matched the spacing of the old wheel ruts in the ancient roads that were built by the Romans for their legions to travel on. Wagons had to match the old wheel rut configuration or risk being destroyed. The wheel spacing was exactly that of a Roman war chariot, which was a military item under standard and specification control. The wheel spacing on a chariot was just wide enough to accommodate the rear ends of two war horses! ("The railroad gauge," n.d., p. 1)

C. MOBILIZATION FOR WAR – THE IMPACT OF STANDARDS & SPECIFICATIONS

The middle of the nineteenth century marked the modern era's process for preparing for war. The era of mobilization was born with the start of the Civil War. Mobilization is the process by which a nation transitions from a normal state of peacetime preparedness to a war-fighting posture by assembling, organizing, and applying its resources for national defense. ("Master mobilization plan," 1988, ¶ 2) The Civil War brought an organized application of resources to prepare, build, and equip mass fighting forces. This nation's volunteer minuteman army, which served the nation well in its infancy, was now defunct. The need for standardization was rampant with no consolidated efforts by either side. ("Mobilization," n.d., p. 3)

In 1917 the United States entered World War (WW) I without stockpiles of equipment or standards for producing them. The military had little experience with industry and often the Army and Navy competed with each other for products, materials, and plant capacity. ("Mobilization," n.d., p. 3)

WW II marked an unprecedented mobilization effort providing for the development, production, and delivery of combat systems and supplies to our troops and Allied forces ("Mobilization," n.d., p. 22). The use of military standards and specifications was widespread including the use of statistical quality control methods. The wartime mobilization needs and tight schedules necessitated the use of statistical

techniques to control and improve quality. Standards for quality control can be traced back to the works of Frederick Taylor in 1875 who introduced the concept of dividing work into manageable tasks. He developed standardized production and assembly methods, which resulted in productivity increases and quality improvements. Assembly operations became more repeatable and less prone to errors. Although standard methods generally provide for increased quality, they risk impeding innovation and continuous improvement, which is vital to growth. The works of Walter A. Shewhart, Harold F. Dodge, and Harry G. Romig of Bell Telephone Laboratories in the first half of the 20th century contributed to the first statistically based sampling standards (vice 100% inspection) for the military during WW II and beyond. (Montgomery, 2001, pp. 8-11)

WW II spawned what Eisenhower coined as the "Military Industrial Complex" which grew as this country mobilized for WW II and prospered during the four decades of the Cold War (Higgs, 1995, ¶ 2). During WW II approximately 20% of the civilian workforce was supporting the defense industry. In 1999, the defense industry employed about 2% of the civilian workforce. (CDI, 2002, ¶ 1)

D. RISK AVOIDANCE THROUGH STANDARDS & SPECIFICATIONS

Following WWII, this country's military posture and doctrine was framed around a known Cold War adversary and threat. We countered this threat with both conventional and strategic military strategies aimed at a potential European ground war and deep sea conflicts. Sea-based and land based strategic weapons provided a necessary deterrent that led to decades of stalemate or détente. The increasing military buildup in the 1950s fueled the U.S. economy, and by 1960 the defense industry accounted for more than half of the U.S. federal expenditures (CNN Interactive, 2002, preface). The Military Industrial Complex was thriving. It continued into the 1960s due to the space race and again in the 1980s as a result of the Reagan buildup.

Our defensive build-up was achieved with an infrastructure of military standards and specifications. They provided proven standards, methods, and practices for design,

build, and testing phases. Risk avoidance through standards and specifications was the norm.

Many believe implementing standards and specifications are costly, and savings could be realized by replacing them with commercial specifications. On the contrary, they were not costly per se, but costly in the manner in which they were invoked. Many times standards and specifications would be invoked in their entirety, instead of properly tailored. This drove up the cost because the contractor had to address blanket requirements rather than the critical ones. In other cases the contractor had to negotiate with the Government on what the real requirements were. The use of proven standards and practices is a good risk avoidance technique. However, it is not proactive, nor does it take advantage of the technological innovations of the commercial marketplace.

Instead of the wholesale cancellation of military standards and specifications in 1994, the better approach would have been to tailor existing military standard and specifications and supplement as necessary as innovations occurred within the defense and commercial sectors. Besides, Dr. Perry's mandate to replace military standards and specifications with commercial ones was accomplished many times by simply rewriting the document in a commercial format and keeping much of the original military content. This was done, not for sake of time, but because the military standards and specifications contained sound standards and best practices. In other cases the military standards and specifications needed updating because they did not contain the latest technological innovations.

In the 1960s and 1970s, DoD outspent the private sector in total Research & Development spending. At the height of the space program the government (including NASA) spent nearly two-thirds of the overall R&D funding. DoD R&D efforts were drivers for technology innovation, ingenuity, and knowledge. Many high technology solutions were transformed into the commercial marketplace. The space program initiated many technological advances that are now common in the private sector including semiconductors, biomedical equipment, and satellite systems. Some feel that today's focused investment in technologies for homeland defense may spawn additional dual use technologies. ("Defense spending," 2002, ¶ 7).

Prior to acquisition reform, a risk awareness culture of risk taking was not needed because defense budgets were large and could sustain the infrastructure of a sizable DoD supplier base, a network of specifications and standards, and investment in R&D. The Cold War ended when our adversary's military-economic infrastructure crumbled and signs of capitalism emerged. With the threat gone, defense budgets were cut drastically in the early 1990s. The DoD infrastructure could not be supported any longer and the time was right for reform. DoD R&D funding was cut and could not keep up with the technological revolution of the commercial marketplace. The demand for electronic components for consumer electronics, telecommunications, and automobiles essentially drove DoD out of the marketplace. DoD contractor mergers resulting from defense cuts left us with a shrinking supplier base signaling the end of the Military Industrial Complex. Even without the formal acquisition reform mandate in 1994, DoD was destined for a revolution in military and business affairs. Limited defense budgets and market forces were driving us to this point.

Today, it is clear that DoD relies on an integrated commercial—military industrial base. However, both markets are motivated by two opposing forces. The military is concerned with executing the mission while keeping our warfighters safe. The commercial market is concerned with making a profit at all costs. It is often difficult to integrate these two opposing forces.

E. GENERAL APPROACH

This research examines how technical risk management has evolved throughout the Navy and determines to what extent technical risk management methods are being used by program managers and other acquisition personnel. A sample of DoN program managers, acquisition professionals, and industry representatives was surveyed to determine attitudes on technical risk management, what methods they are using, and what training they have received. Members from all three Navy Systems Commands (SYSCOM), specifically NAVSEA, Space and Naval Warfare Systems Command (SPAWAR), and Naval Air Systems Command (NAVAIR) were surveyed. The results will be used to assist Office of the Assistant Secretary of the Navy, Research,

Development and Acquisition, Acquisition and Business Management (ASN(RD&A)ABM) in writing future risk management policy and guidance for the Navy.

F. RESEARCH QUESTIONS

This thesis will address the following research questions:

- What is the history of technical risk management?
- What are the advantages and disadvantages of technical risk management?
- What are the current practices for technical risk management within DoN program management offices?
- Have DoN program management offices implemented the technical risk management guidance of NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*? What guidance documents are they using?
- What are program management offices' opinions of technical risk management?
- What are some potential solutions to minimize technical risk?
- How does a systems engineering framework avoid or minimize technical risk?
- How do decisions made today affect tomorrow's products?
- What are other sources of technical risk management best practices, lessons learned, and metrics?
- What are some sources for technical risk management methods & techniques and what do they teach?

G. ORGANIZATION OF THE THESIS

This thesis in organized into four chapters. Chapter I provides an introduction to acquisition reform and describes its relationship to a risk awareness culture change within the acquisition community. It also discusses the origin and evolution of risk avoidance methods prior to acquisition reform. Chapter II defines technical risk management and describes methods & techniques currently used within the Navy. Chapter III describes the research methodology and the survey tool used to solicit opinions and information from program managers, their staff, and other acquisition professionals. It also provides

the survey results and analyzes the results for significant trends. Chapter IV provides a summary of the research with conclusions.

II. TECHNICAL RISK MANAGEMENT METHODS

A. THE ORIGIN OF TECHNICAL RISK MANAGEMENT

During the middle of the Cold War era the space race was a welcomed preoccupation of both political & military leaders and the public at large. From the moment that Sputnik I was launched on October 4, 1957, this country was determined not to let our Cold War adversary gain supremacy of space. The National Aeronautics and Space Administration (NASA) was formed on 1 October 1958 as a result of the "Sputnik crisis of confidence" and immediately began working on human space flight ("NASA history," 2002, ¶ 1). NASA's mission was expedited when President Kennedy uttered the following words to a joint session of Congress on May 25, 1961: "I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the earth." (JFK Library, 2002, chap. IX, ¶ 5)

The very success of the Mercury, Gemini, and Apollo manned space flight programs can be attributed to process discipline and rigor implemented through a regimen of strict standards and specifications and contractor oversight. The oversight consisted of many checks and balances and layer upon layer of inspections according to Douglas Patterson, former ASN(RD&A) Technical Director, who was involved in the Apollo program (D. Patterson, personal communication, August 8, 2002). NASA was risk averse and managed risk by trying to avoid it altogether with high reliability and redundant systems. Those systems, subsystems, and components that could not achieve high reliability were classified as High-risk items and risk mitigation actions were taken. Let's examine this risk avoidance culture in more detail and discuss how a catastrophic event caused this agency to rethink how they practiced risk management.

Historically, NASA practiced risk avoidance, relying on strict oversight, manufacturing and assembly process controls, use of design safety factors, and criticality analyses (e.g., a failure of a "criticality one" component could lead to loss of vehicle and the crew). This was particularly the case until the Challenger disaster. Why? In the

early 1960s various mathematicians and consultants using Probabilistic Risk Assessment (PRA) techniques calculated that there would be a very small probability of success of reaching the moon. NASA feared these results would frighten the public and adversely impact congressional funding for the program. As a result, NASA banned the use of PRA methods and turned their focus on risk avoidance.

Willis J. Willoughby, Jr., Director of Product Integrity for the Apollo Program Reliability, Maintainability, and Quality Assurance (RM&QA), was responsible for Apollo's reliability record. He was instrumental in institutionalizing a focus on engineering fundamentals and discipline within NASA, creating a risk avoidance and risk abatement management style, which was further strengthened after the 1967 Apollo I disaster. After a brilliant career with NASA, Mr. Willoughby came to the Navy bringing with him the concepts he developed for NASA. NASA continued down the path of risk avoidance from the end of Apollo, to the Explorer program and the start of the earth orbiter shuttle program. Somewhere along the way in the 1970s NASA management style began to change, and they lost the recipe for accountability, critical management level checks and balances, and process rigor. Then came the Challenger accident and a wake-up call for NASA. As a result, a realistic assessment of risk was needed on the space shuttle program. Although the failure mechanism was a solid rocket booster O-ring, there were a number of underlying causes associated with the lack of discipline and process rigor. Management failures including poor communication, schedule pressures, political pressures, and incentives to launch foretold an inevitable hardware failure. This is an example where process risk leads to product risk. NASA realized a more proactive method was needed to assess risk.

By this time PRA methods were commonplace in the Nuclear Power Industry, so NASA took another look at these proven methods used in mission/safety critical applications. In the days of Apollo, probabilistic assessment methods were not completely avoided. According to Mr. Patterson, these methods were used selectively for special studies, critical items, and single points of failure. Because NASA depends heavily on public relations to keep the funding lines flowing, the agency has been willing to take a little more risk. Cornell and Fischbeck state, "Soon after the shuttle's

introduction, the agency shifted from a conservative attitude of 'launch if proven safe' to an attitude of 'launch unless proven unsafe'." (Pate-Cornell & Fischbeck, 1994, p. 75) The managers generally shared this optimism more than the engineers and scientists working directly with the systems (Pate-Cornell & Fischbeck, 1994).

DoD practiced similar risk avoidance techniques as NASA prior to 1985. Like NASA, DoD used their network of military specifications and standards to avoid risk through the application of proven (and Low risk) standards and practices. DoD and DoN policy lacked risk management requirements, and there was little guidance for program managers. Technical performance measures and reactive, problem solving methods were used to control risk. "Historically, Department of Defense (DoD) and Department of the Navy (DoN) Program Managers have used cost, schedule, and performance parameters to exercise control over and measure the success of their programs." (ASN(RD&A)ABM, 1997, p. 1) These were mainly reactive methods. It took a cultural change initiated by Willis J. Willoughby, Jr. in 1985 and further influenced by acquisition reform in the 1990s to instill the importance of early identification of technical risk.

A survey of Acquisition Category (ACAT) I through IV program managers in 1997 by ASN(RD&A)ABM found an increasing awareness of technical/performance risk as the driver for cost, schedule, and performance outcomes on an acquisition program. This survey also found more proactive risk management efforts taking place within the acquisition community, as well as greater emphasis in policy documents, such as DoD and DoN 5000 series. Guidance documents were also becoming available from DoD and DoN and also available in the *Defense Acquisition Deskbook*. The results of the survey included the following observations:

- 50% of the programs surveyed did not have risk management plans
- Few programs offered risk management training
- While all ACAT I programs surveyed contained a contractual requirement for risk management, few ACAT II, III, or IV programs had such a requirement
- None of the programs surveyed used award fee scoring criteria to incorporate risk management

- Only three programs (all ACAT I) use independent risk assessment teams ((ASN(RD&A)ABM, 1997, p. 1)

A defining moment in the history of the Navy's application of risk management methods occurred when RADM Isaac Kidd stole Mr. Willoughby from NASA in 1973 bringing him to the Navy as Deputy Chief of Navy Material. ("Willis Willoughby," 1998, ¶ 3) Mr. Willoughby brought with him the concepts he developed while working for the Apollo program in the Office of Manned Space Flight during its heyday. Mr. Willoughby made significant contributions to the Apollo program. NASA's collection of history ("Preparation for flight," 1967, March 14) recalls Mr. Willoughby's appointment to a special review team chartered to audit the quality control and inspection practices of Apollo spacecraft operations at both government and contractor activities. This special audit team was formed as a result of the 1967 Apollo I fire and accident investigation that killed astronauts Gus Grissom, Roger Chaffee, and Edward White ("NASA historical reference collection," 2002, ¶ 2). Mr. Willoughby was also instrumental in bringing Apollo 13 back to earth safely. ("Willis Willoughby," 1998, ¶ 3)

Mr. Willoughby brought a culture change to the Navy. His philosophy was based on an adherence to engineering fundamentals and discipline. He believed in designing reliability into the product instead of inspecting it in. He brought to the Navy improved weapon and combat system reliability, readiness, improved production quality, and minimum life cycle cost. He preached early identification of technical risk so it can be mitigated rather than taking a wait and see what happens approach. He believed technical risk is the driver behind all other risk, so it must be addressed early in the acquisition life cycle.

It is interesting how the only two tragedies in the history of manned space flight resulted in a greater emphasis on risk analysis and management. The 1967 disaster had an indirect impact on the Navy's application of engineering discipline and process rigor as a result of Mr. Willoughby's experience and lessons learned from his NASA tour. The Challenger disaster in 1986 forced NASA to supplement its risk avoidance approach

through standards and specifications with more proactive probabilistic methods. Although on the right path, the Navy has not reached a similar point of integration.

B. RISK MANAGEMENT FRAMEWORK

Risk management is a process. As with any process, it can be flow charted to provide a graphical depiction of the relationships and interfaces between the major components. Risk management can be conducted using different approaches. Regardless of the risk management strategy taken, a basic foundation or framework exists. Figure 2 illustrates the key components of the risk management process. This framework applies to any risk management approach.

1. Risk Areas

Typically, risk is categorized as technical or non-technical risk. Technical risk can be further broken down into process and product risk. Process risk is directly associated with the critical engineering processes and disciplines used to design, test, and fabricate a product. A product is defined as a hardware or software item. A product risk is hardware, software, and technology specific and relates to the performance of the product itself as opposed to the process used to create the product. Technology risks associated with leading edge products or technologies yet to be proven are also grouped under the product risk area unless the technological challenge is an engineering or manufacturing process. Often, technical risk drives cost, schedule, and performance risk, and this is the reason why technical risk should be addressed first and early in the acquisition life cycle. Non-technical risk is the category reserved for contracting, program management, and programmatic related risk events. Note, occasionally a risk event may fit the definition of multiple risk areas. When this occurs the assessor should assign the risk event to the most appropriate category with assistance from the IPT lead or Risk Manager if so desired.

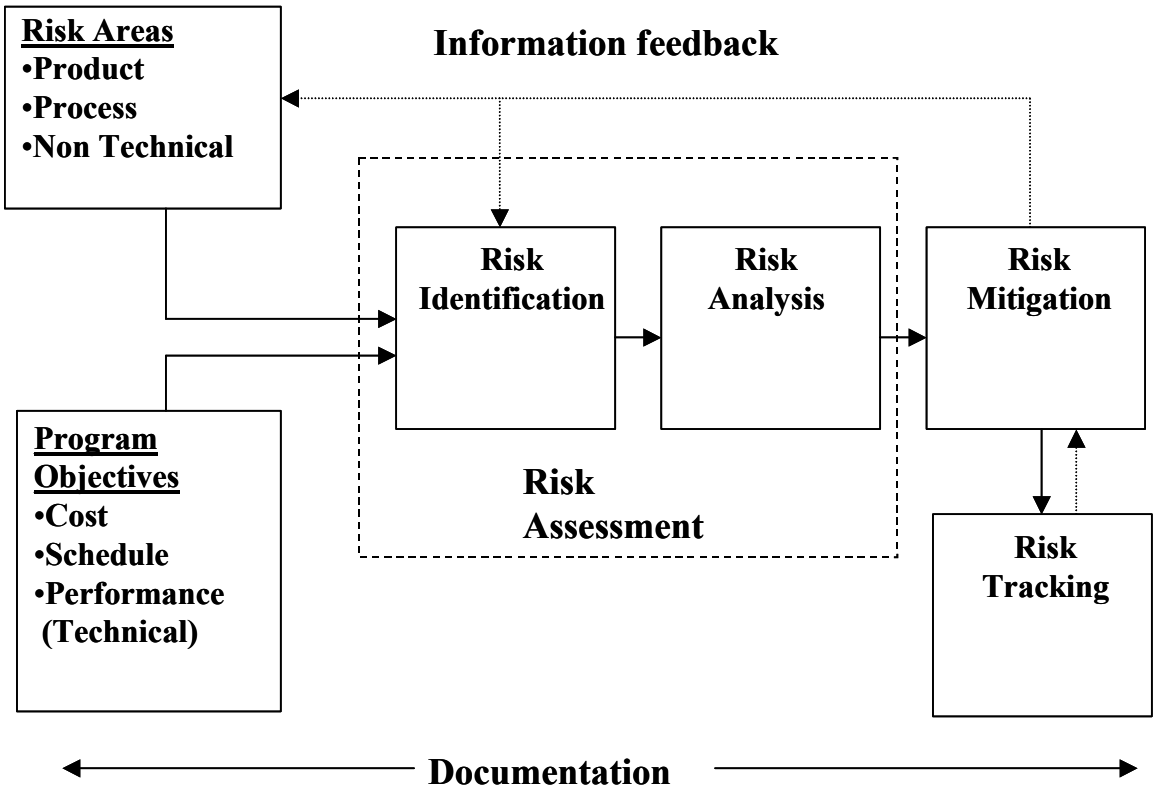


Figure 2. Risk Management Process. From (SURTASS, 2002, p. 10)

2. Program Objectives

The most common program objectives the program manager is concerned with are cost, schedule, and performance parameters. This triad is often referred to as the "Iron Triangle" of project management as shown in Figure 3 (American Graduate University, 1998). It is important to note that cost, schedule, and performance are not mutually exclusive, but interrelated. If one is affected, the others will also be affected. Think of the triad as a triangle made from a rubber band. At each point is one of these parameters. Think of each parameter pulling against the other, so the triangle is a continuously undulating shape. Throughout the acquisition cycle, the program manager is continuously conducting trade-offs between these three parameters in order to arrive at a proper balance among them. Historically, the success of a program manager was

measured based on cost and schedule performance, with performance often traded off to improve cost and schedule.

Today, with the increased focus on systems engineering, a balanced solution among cost, schedule, performance, and risk is the objective. The three program objectives depicted in Figure 3 may also be supplemented as needed. Some programs have elevated environmental, safety, and security parameters to the program objectives list.

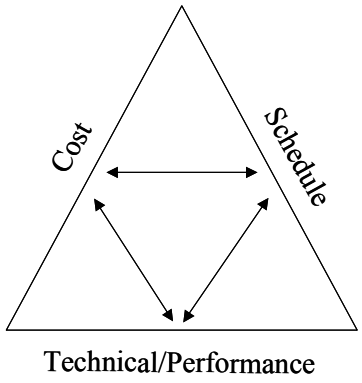


Figure 3. The Iron Triangle of Project Management. From (Amer. Graduate Univ., 1998)

3. Risk Assessment

The term risk assessment is often used interchangeably with risk analysis. However, the most common interpretation is that risk assessment consists of two components: risk identification and risk analysis. Risk identification is the act of identifying risk within risk areas. It involves documenting the risk appropriately. Risk analysis follows risk identification and is the process of classifying the risk. Classification consists of assigning a risk level (e.g., Low, Moderate, High) to the risk using any number of classification techniques available, some which will be discussed later. Risk levels are assigned in order to prioritize handling. In an ideal world, risk mitigation actions are taken on all identified risks. In today's environment of limited resources, usually only the High and Moderate risks are mitigated.

4. Risk Mitigation

Risk mitigation, also known as risk handling, is the process of identifying, analyzing potential options, selecting, and implementing risk mitigation solutions for the identified risk. Mitigation is defined as reducing a risk to an acceptable level. It does not necessarily mean eliminating the risk, that would be the ideal world once again. Risk mitigation planning is conducted and a Plan of Action and Milestones (POA&M) is documented for the selected approach. Generally, the risk level and the POA&M is documented on the same risk form with the risk description and in many cases part of a risk management database. A risk mitigation POA&M should be loaded into the program's integrated master schedule and Work Breakdown Structure (WBS) to assure resources are planned and loaded for risk mitigation activities.

5. Risk Tracking

Risk tracking is the process of monitoring the risk mitigation progress of the POA&M. As part of this process, the effectiveness of risk handling efforts is assessed to a collection of performance measures. Risk tracking requires periodic risk assessment follow-up and a relook at lower level risks not part of the initial risk mitigation planning effort. Low risks can escalate, so a periodic reassessment of Low risks is warranted. Participation in risk review boards is an excellent way to stay informed as part of the risk tracking/monitoring effort.

6. Information Feedback

The success of the risk management process relies on information feedback throughout the process. Feedback of risk mitigation efforts to the beginning of the risk management process flow allow us to iteratively reassess and adjust the risk level as mitigation actions are taken (or not taken). Feedback to the risk area element may cause another risk of a different category to be formed. We know that process risk leads to product risk; thus ineffective process risk identification could lead to a new product risk.

7. Documentation

Throughout the entire risk management process properly documenting the risk event is critical. Documentation includes recording risks and associated risk mitigation plans, as well as reporting risk status to management. As a minimum, the following fields are recommended to properly record a risk: 1) risk tracking number, 2) risk title, 3) risk description, 4) risk level, 5) rationale for risk level, 6) risk mitigation PO&AM for Moderate and High risks, 7) risk mitigation actions completed, and 8) risk owner. The documentation should include all supporting documentation associated with the risk and mitigation plans and results. Many programs use electronic risk databases to capture this information. Databases allow for easy tracking and reporting of risk status. Some smaller programs still use manual risk identification forms. A key output of the documentation process is the reporting of risk status and results to management.

C. RISK IS EVERYWHERE

There is risk in every program. This is a fact that program managers must accept. It is impossible to avoid risk in the complex process of weapon system development, modification, or procurement. The complexities of hardware and advanced software products lead to program risk. Risk is inherent in the development process, the modification or upgrade of existing products, and the use of Commercial-Off-The-Shelf (COTS)/Non-developmental Items (NDI). Because risk is so prevalent in everything we do, the key to success is the early identification of risk so mitigation actions can be taken to reduce the risk to acceptable levels. "Risk that is known, monitored, and adequately mitigated seldom interferes with successful product development." ("Methods & Metrics," 1994, p. 3)

D. THE EVOLUTION OF TECHNICAL RISK MANAGEMENT METHODS IN THE NAVY

In the late 1970s and early 1980s many of our aircraft and ship systems were unreliable and not maintainable. For instance, the Navy was ready to proceed with full

development of the F/A-18 Hornet in the late 1970s. However, initial reports from the Fleet indicated that the aircraft required servicing after only 30 to 45 minutes in the air. Mr. Willoughby, while Deputy Chief of Navy Material Command for Reliability, Maintainability & Quality Assurance, insisted that all F/A-18 contracts include provisions for reliability and maintainability instead of just flight performance. As a result, the F/A-18 entered Initial Operating Capability (IOC) with greater reliability than many mature systems and took less than half as many maintenance man-hours as other aircraft. In the first operational deployment the aircraft would end a day of flying still able to fly while the F-14s and A-6s were already in for service. In addition, the F/A-18 engine could be changed in 20 minutes. As a comparison, the A-4 Skyhawk flown in Vietnam required its tail to be removed before an engine could be changed. (Clark & Johnson, 2002, ¶ 1-4)

In 1981, the MK 92 fire control system was experiencing performance problems in the Fleet, so an aggressive program to improve its performance and reliability in clutter and electronic counter-measure environments was launched. MK 92 provides FFG 7 class frigates and other surface combatants with a weapons control system for use against air and surface targets (Military Analysis Network, 2002a, ¶ 1-2).

The MK-15 Phalanx Close In Weapon System (CIWS) was another system that had low operational availability. MK 15 is a fast-reaction, rapid-fire 20-millimeter gun system that provides U.S. Navy and Allied ships with a final, short-range defense against anti-ship missiles and fixed wing aircraft that have penetrated other Fleet defenses. (Military Analysis Network, 2002b, ¶ 1) This system was rushed to the Fleet to provide close in anti ship cruise missile defense as a result of the sinking of Britain's *HMS Sheffield* by Argentinean air attacks from fighter planes using Exocet air to surface missiles in the Falklands War ("Chronicle of the Falklands," n.d., May 4). CIWS has been deployed on nearly every class of ship since the early 1980s.

There were many other troubled systems with poor performance and reliability problems, as well as high maintenance burdens in the early 1980s. As the complexity of weapons and combat systems grew, some soothsayers believed the reliability of systems would be impacted negatively, blaming the complexity for poor readiness.

In 1985 a Defense Science Board (DSB) Study, chaired by Mr. Willoughby, deliberated the issue of complexity versus readiness and found little evidence that increasing complexity of new DoD weapon systems was the result of recent trends in poor readiness. Rather, the probable cause was inadequate engineering and manufacturing disciplines during the design, development, and production of the system. The DSB was comprised of government and industry members. The team postulated that once rigorous and disciplined engineering practices were employed and institutionalized, the risk of deploying unsuitable weapon systems would be Low and the time in the acquisition cycle would be reduced. It is interesting to note that back in 1985 DoD realized the acquisition cycle times were too long and desired methods to shorten these cycles. This is the same challenge we are facing today. In 1985, the solution was more rigorous engineering discipline and processes during the development phases prior to a Milestone III production decision. (DoD 4245.7-M, 1985, pp. 1-8)

Given the number of acquisition programs with poor reliability, burdensome maintenance, and supportability issues a DSB Task Force was formed under the auspices of the DSB to develop a set of disciplines and controls for application during design, test, and production activities. The government and industry representatives on the Task Force came up with a list of templates that acquisition programs could follow to minimize program risk. These templates were nothing more than critical engineering disciplines and processes for use in describing Low risk programs. They are also key components of the systems engineering process. This collection of templates was published in September of 1985 as DoD 4245.7-M, *Transition From Development To Production…Solving the Risk Equation*, by the Assistant Secretary of Defense for Acquisition & Logistics. They soon became known as the "Willoughby Templates," after Mr. Willoughby, DSB Task Force Chairman. Figure 4 provides a high level look at the Templates, which have been supplemented by the Best Manufacturing Practices Center of Excellence (BMPCOE) since their initial release. The shaded templates depict 18 new templates that have been added by BMPCOE.

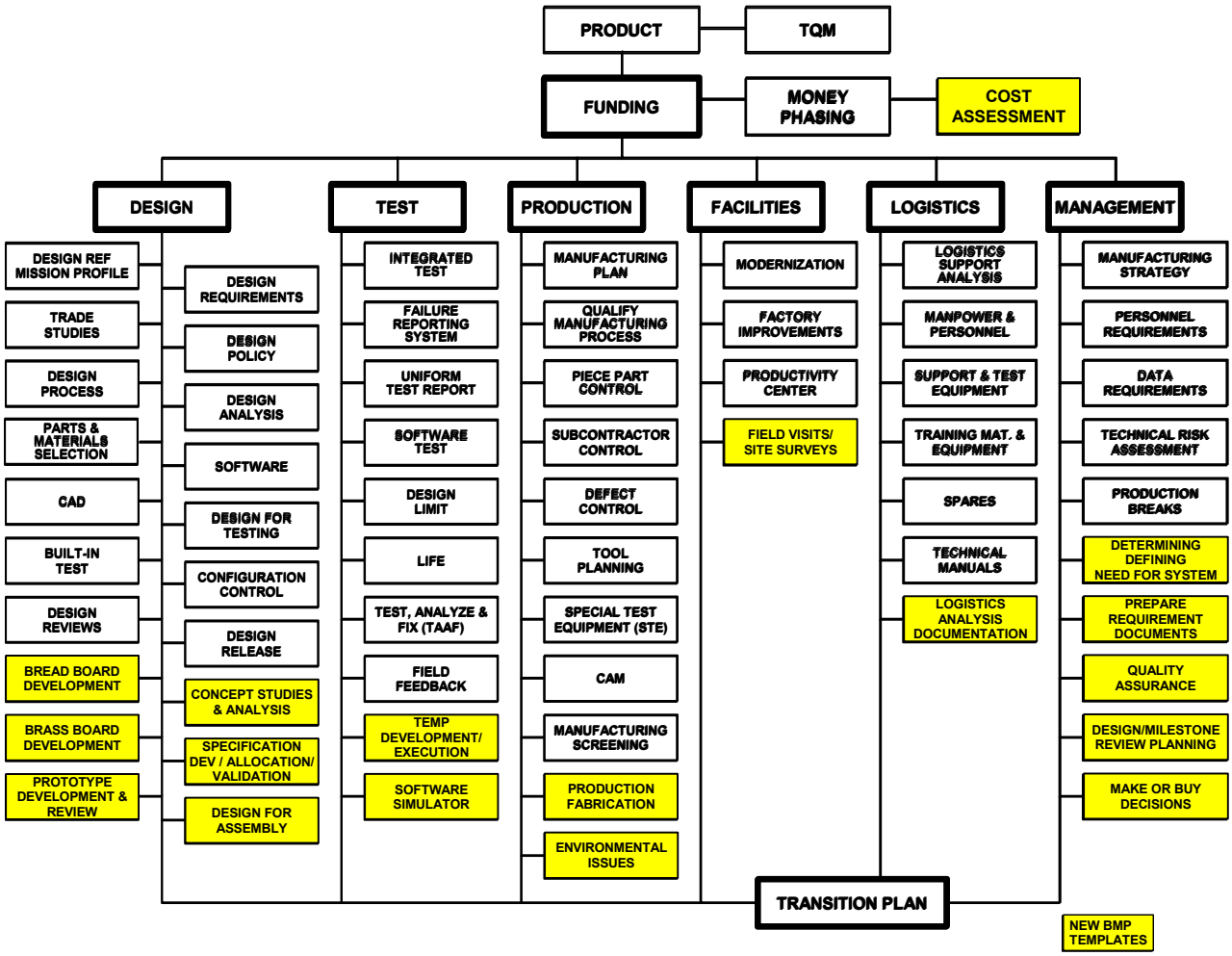


Figure 4. Willoughby Templates. After (DoD 4245.7-M, 1985, p. 8)

Because of Mr. Willoughby's many contributions in this field, he is considered the father of reliability for his ruthless advocacy of product integrity disciplines throughout his career ("Willis Willoughby," 1998, ¶ 1). Mr. Willoughby's release of DoD 4245.7-M to the acquisition community marked the beginning of technical risk management within DoD and the Navy. He also drafted a number of acquisition standards and guidance that have improved Fleet readiness and reduced life cycle costs. He was responsible for the creation of many innovative acquisition management products and tools, including the Best Manufacturing Practices (BMP) program and the Program Manager's Workstation. The BMP program is a knowledge repository of industry and government best engineering practices which is available free of charge to both government and industry in order to promote sharing of best practices. Program Manager's Workstation (PMWS) is an electronic suite of software tools designed to provide acquisition know-how, best industry practices, and a templates-based technical risk management software program for use by acquisition professionals. Together these tools provide a comprehensive knowledge information, measurement, and risk management system based on critical engineering processes and best practices through all phases of the product development life cycle. For these reasons, this author will always considered Mr. Willoughby the father of technical risk management.

In 1998 Willis J. Willoughby, Jr. was inducted into the Navy Acquisition Hall of Fame as an Acquisition Pioneer. The Navy Acquisition Pioneer program was established in 1997 by ASN(RD&A), John Douglass, to recognize the achievements of past, present, and future acquisition leaders in the Navy and Marine Corp ("Willis Willoughby," 1998, ¶ 1). He was nominated by both NAVAIR and NAVSEA for a lifetime of achievement and ruthless application of product integrity disciplines to many Navy and Marine Corps systems. Some of the greatest operational successes during the Gulf War, such as the F/A-18 Hornet, Tomahawk and HARM missiles, were the result of Mr. Willoughby's attention to engineering discipline and process rigor (Dalton, 1998, p.2). The Honorable John H. Dalton, Secretary of the Navy, presented the award to Mr. Willoughby and remarked, "it is no secret he built quality and engineering competence into every program he touched…programs like the S-3A, CH-53B, Harpoon, SPS-49, the AEGIS system and

many more." (Dalton, 1998, p.2) Mr. Willoughby's son, Brian, is following in his father's footsteps and carrying on the product integrity tradition since his father's death in 1999. In regards to his father's work, Brian Willoughby stated, "He started out in the RM&QA business, what he did never really changed, it is just called technical risk management today." (Brian Willoughby, personal communication, August 12, 2002)

Although managing risk for all aspects of a program is critical, technical risk is the most important area of risk management because technical risk is the driver behind all other program risks including cost, schedule, and performance risks. Technical risk management assesses the implementation of critical engineering processes and disciplines up front and early during the acquisition life cycle. These disciplines are also characterized as engineering fundamentals. If these critical engineering disciplines are not implemented, then there is risk that products (hardware/software) will be adversely impacted. This relationship between Process and Product is characterized by the following statement: Unmitigated Process risk leads to Product risk. Both government and industry experiences have proven that basic disciplined design, test, and production practices are critical for Low risk acquisitions. Program risks are often the result of poor management decisions regarding the application of engineering fundamentals. Therefore, technical risk management also focuses on sound management decisions based on the assessment of risk.

Risk assessment techniques, a subset of risk management, were first used to measure how well an acquisition program had implemented critical engineering disciplines. Critical processes are interrelated and interdependent which means a failure to do well in one area may adversely impact other areas.

Unfortunately, technical risk management and the importance of controlling critical technical processes have generally not been well understood within the DoD acquisition community. The acquisition process has traditionally focused on cost and schedule issues, i.e., on time and within budget, instead of performance in-service. "Its milestone decision points are unrelated to the industrial processes and the transition between development and production in the factory." (NAVSO P-6071, 1986, p. 5) As a result, much of the DoD and DoN policy and guidance on risk management has taken a

technical risk management approach. (NAVSO P-3686, 1998, pp. vii, 19) Program managers and other acquisition personnel must understand the technical and industrial processes involved in the acquisition process in terms of best practices and lessons learned. (NAVSO P-6071, 1986, p. 7)

The critical engineering disciplines required for Low risk programs, such as those described in DoD 4245.7-M, are quite valid in today's acquisition environment. These disciplines are key systems engineering disciplines, and the systems engineer or architect should have direct responsibility to ensure these critical disciplines are implemented in new acquisitions. Systems undergoing major modifications, upgrades, and reprocurements should also apply systems engineering disciplines. Today, we are fighting the same battle of trying to shorten the acquisition cycle. We are challenged by trying to support legacy systems and life extension initiatives for programs beyond their original design life. The prevalent use of COTS and associated short technology refresh cycles has led to Diminished Manufacturing Sources & Material Shortages (DMSMS). The short commercial product development cycle is not in sync with DoD's long acquisition cycles. Despite nearly 10 years of acquisition reform, acquisition cycles are still too long. Achieving interoperability between U.S., Allied, and coalition systems is a key objective of the latest DoD 5000 series documentation. In order to achieve this interoperability, there has been an increased emphasis on systems engineering and associated disciplines. Systems engineering includes the same critical engineering disciplines mentioned in the 1985 templates.

Risk assessment is still used to measure how well programs are doing with the implementation of systems engineering disciplines. What have improved over the course of 17 years are risk awareness and the integration of risk management into the program manager's tool kit. It is a management discipline now, not just an assessment tool. In addition, the risk management approach is more proactive where the previous technical risk assessment efforts were somewhat reactive due to the emphasis on the transition to production phase. Often program managers and other acquisition personnel used the Willoughby Templates to conduct a risk assessment just prior to a Milestone (MS) III Production decision. The risk assessment was usually done as part of the Production

Readiness Review (PRR). Later, this practice was modified by some program managers to an incremental risk assessment process throughout Engineering and Manufacturing Development (EMD). It was typically implemented through the use of incremental PRRs with a final wrap-up PRR a few months before the MS III Defense Acquisition Board (DAB) or equivalent meeting. This evolution from risk assessment to risk management occurred to inject a more proactive approach to risk identification and mitigation. Risk assessments conducted just prior to MS III during the transition to production phase were purely reactive and much too late in the acquisition life cycle to affect cost effective change.

This improvement was the direct result of acquisition reform back in 1994. With the elimination of military specifications and standards, program managers no longer had a risk avoidance method. With the use of commercial specifications and contractor internal processes, program managers lost insight into their acquisition programs including much of the engineering process rigor. Program managers were forced to supplement their tool kit with a method to gather insight and proactively mitigate potential risks.

There has also been a policy shift over the last 17 years with an increased emphasis on risk management in the DoD 5000 series acquisition program policy documentation, facilitated by acquisition reform initiatives. If it were not for acquisition reform policy, we might never have seen such an increased focus on risk management.

Today, risk assessment is a key component of an acquisition program's overall risk management program. Risk assessments are conducted as early as possible and are applied continuously throughout the acquisition life cycle on successful programs.

1. Technical Risk Management Guidance

The following paragraphs will highlight some of the best guidance documents and tools for technical risk management. The Navy leads the other Services in setting the standard for technical risk management methods development and the publication of guidance to educate its workforce. Although the following documents and tools were for

the most part created by Navy acquisition professionals in partnership with selected industry representatives, the resultant products are applicable to the entire DoD acquisition community.

a. DoD 4245.7-M

DoD 4245.7-M, a.k.a. the Willoughby Templates, contains a collection of 48 templates. Each template describes an area of risk inherent in the design, test, and productions processes and then specifies technical methods for reducing that risk. Additional templates address other critical areas since program risk is also associated with funding, facilities, management issues, and the transition plan for the production phase. The entire network of Templates is arranged in a logical sequence as seen from a program manager's viewpoint. Funding is presented first because it influences every other template in the document. (DoD 4245.7-M, 1985, p. 5)

Despite its age, DoD 4245.7-M is timeless. Today, this document can be found in the *Defense Acquisition Deskbook*, as well as on many acquisition related web-sites. These templates are used by the Best Manufacturing Practices (BMP) Program to conduct BMP surveys of government and industry facilities/contractors. This collection of 66 templates is dynamic and continues to be supplemented as best practices and lessons learned are discovered which further reduce the technical risk of military and commercial product development and production.

This document is often used as a guideline by risk assessment teams to evaluate how well a contractor or government activity has implemented critical engineering (best practice) disciplines. It is the original technical risk assessment guiding document and remains invaluable. The 48 original templates have served as a foundation for technical risk on which additional critical engineering disciplines have been built.

b. NAVSO P-6071 Best Practices Manual

Released in March of 1986 as a Navy guidance document, NAVSO P-6071, *Best Practices – How to Avoid Surprises in the World's Most Complicated Technical Process*, was a follow-on to the Willoughby Templates. Mr.

Willoughby acting as Chairman, Defense Science Board Task Force, Transition from Development to Production, was responsible for the publication of this guidance manual. This manual was written as a working tool in a user friendly, easy to read format. This manual, as well as DoD 4245.7-M, was conceived by a joint government/industry team. It contains best practices and industrial processes used within government and industry. For each DoD 4245.7-M template area, the manual contains a collection of checklists, traps, and pitfalls. It illustrates common mistakes that past and current defense programs have made which have led or will lead to technical risk. It contains a chart, which compares the consequences of current approaches vice the best practice approach. For purposes of this thesis, a best practice is defined as a critical engineering discipline that must be in place for a Low risk program. Finally, the manual contains a checklist to aid the acquisition professional in implementing a best practice approach and provides a list of assessment questions that a reviewing authority would ask when evaluating whether or not the best practice has been implemented. You may ask, what is "the World's Most Complicated Technical Process?" Why it is weapon system design, test, and production! (NAVSO P-6071, 1986, pp. 2, 5, 11)

c. Methods & Metrics for Product Success

In July of 1994 in the middle of the year of reformation and Dr. Perry's mandate for acquisition reform, ASN(RD&A) released a guidance document for technical risk management called *Methods & Metrics for Product Success*. Once again, Mr. Willoughby had a hand in additional technical risk management guidance performing as lead editor for this document in his position as ASN(RD&A) Deputy for Product Integrity. This document established a methodology and process flow for conducting a technical risk assessment, which will be discussed later. It also provided Measures of Effectiveness (MOE) or metrics for the design, test, and production templates contained in DoD 4245.7-M and NAVSO P-6071. ("Methods & Metrics," 1994, pp. iii-iv) Thus, Navy technical risk management guidance continued to build on the nearly 10 year old Willoughby Templates. *Methods & Metrics* relied on an approach for technical risk management discussed specifically in Dr. Perry's 10 tenets for IPPD. The 10th IPPD tenet states,

> **Proactive Identification and Management of Risk** - Critical cost, schedule and technical parameters related to system characteristics should be identified from risk analyses and user requirements. Technical and business performance measurement plans, with appropriate metrics, should be developed and compared to best-in-class industry benchmarks to provide continuing verification of the degree of anticipated and actual achievement of technical and business parameters. ("IPPD definitions," 1995, ¶ 2)

As evident by this quote, Dr. Perry is advocating that technical processes with associated metrics be established and compared to industry benchmarks (i.e., best practices). This is exactly the approach *Methods & Metrics* takes by developing a set of metrics called MOEs for the critical template areas already well established in previous guidance. The objective is to provide some measurable risk assessment criteria to a traditionally subjective process. "Product success depends upon using proven technical management methods along with established technical metrics during the entire development effort." ("Methods & Metrics," 1994, p. 3) A risk assessment conducted to the guidance of the Willoughby Templates was based on the subjective assessment of the amount of variance between the current approach and best practice. The amount of variance was classified as Low, Moderate, or High. These ratings were based on a subjective assessment by knowledgeable subject matter experts. *Methods & Metrics* provided additional benefits associated with its methodology to the acquisition professional including: 1) communication of program status to management, 2) feedback of measurable results to team leaders concerning the application of key disciplines, 3) a method to assess and measure subcontractor and vendor performance, and 4) support for systems engineering, concurrent engineering, and IPPD initiatives. ("Methods & Metrics," 1994, p. iv)

d. Program Manager's Workstation (PMWS)

The Program Manager's WorkStation (PMWS) is an electronic knowledge information system, which is comprised of a suite of tools designed to assist the acquisition professional. It consists of three tools, namely the KnowHow Database, the Technical Risk Identification and Mitigation System (TRIMS), and the BMP Database.

These tools complement each other and provide a comprehensive acquisition and technical risk management knowledge information system "providing users with the knowledge, insight, and experience to make informed decisions through all phases of product development, production, and beyond." (BMP, n.d., overview). PMWS is available to government, industry, and academia for no charge via BMPCOE's Web Site at http://www.bmpcoe.org. The tools can be run on-line, downloaded to a local hard drive, or ordered on a CD.

The KnowHow database provides an excellent repository of acquisition knowledge and guidance documents. It is an electronic library of technical handbooks, guidelines, and publications, which span a number of acquisition and engineering topics. For example, a quick search of the KnowHow database on key words "value engineering" would result in a number of guidance documents on how to create a value engineering program. (BMP, n.d., knowhow)

The BMP Database contains over 2,500 best practices that have been verified and documented by an independent team of experts during BMP surveys of government and industry activities. Each best practice entry in the database provides basic background, process descriptions, metrics, and lessons learned, and a point of contact for further information. (BMP, n.d., BMP database) The best practices identified in this database provide a critical component of the qualitative technical risk assessment process. In order to determine if a risk exists on a program, the qualitative risk assessment process requires a comparison between current program practice and best practice. The amount of variance determines the risk level. Thus, BMP is an excellent (free) source of best practices information.

TRIMS is an automated technical risk assessment and management tool that allows the user to identify, quantify, track, and report program technical risks and risk mitigation activities. TRIMs applies to all phases of the acquisition life-cycle. Originally conceived by Mr. Willoughby as a way to automate the assessment criteria of his templates, it has grown to include the assessment questions from NAVSO P-6071, the measures of effectiveness from *Methods & Metrics for Product Success*, and criteria from the Carnegie-Mellon Software Engineering Institute (SEI) Software Risk Engineering

(SRE) Model. The TRIMS tool utilizes a framework based on the original Willoughby Templates plus the new template areas added by the BMP program. (Note: TRIMS presently provides several knowledge bases for use in risk assessments. The Systems Engineering knowledge base is the broadest and most widely used which is based on the Willoughby Templates. There is also a Software Design knowledge base for use by software-intensive programs and an Interoperability knowledge base.) Each template area has a number of assessment questions associated with it requiring a Yes or No answer. It asks the minimum number of questions, typically 5-10, needed to assess technical risk and promote dialog among program team members. TRIMS allows the user to create a POA&M for each question if the activity is deficient (i.e., risky) in that area. TRIMS includes over 500 assessment questions which continues to grow as lessons learned are added to the database. An abbreviated sample of assessment questions is shown in Figure 5 for two template areas.

Many users tailor the TRIMS tool prior to using. Template categories, template areas, and assessment questions can be tailored. This is highly recommended as not all template areas apply to every program and the current phase. Unique template areas and assessment questions can be added by the user to more closely align the tool with specific aspects of the program/product.

TRIMS provides links within the tool to the KnowHow and BMP databases. Thus, the user can search these associated databases for best practices for a particular area. TRIMS, along with the other two components of the PMWS, has also been incorporated into the *Defense Acquisition Deskbook*. The use of PMWS was taught to all attendees of the 14 week Advanced Program Management Course at DSMC until 2002 when the curriculum was changed. PMWS is now taught in the DAU Advanced Production and Quality Management course. (BMPCOE, 2000, pp. 1-2)

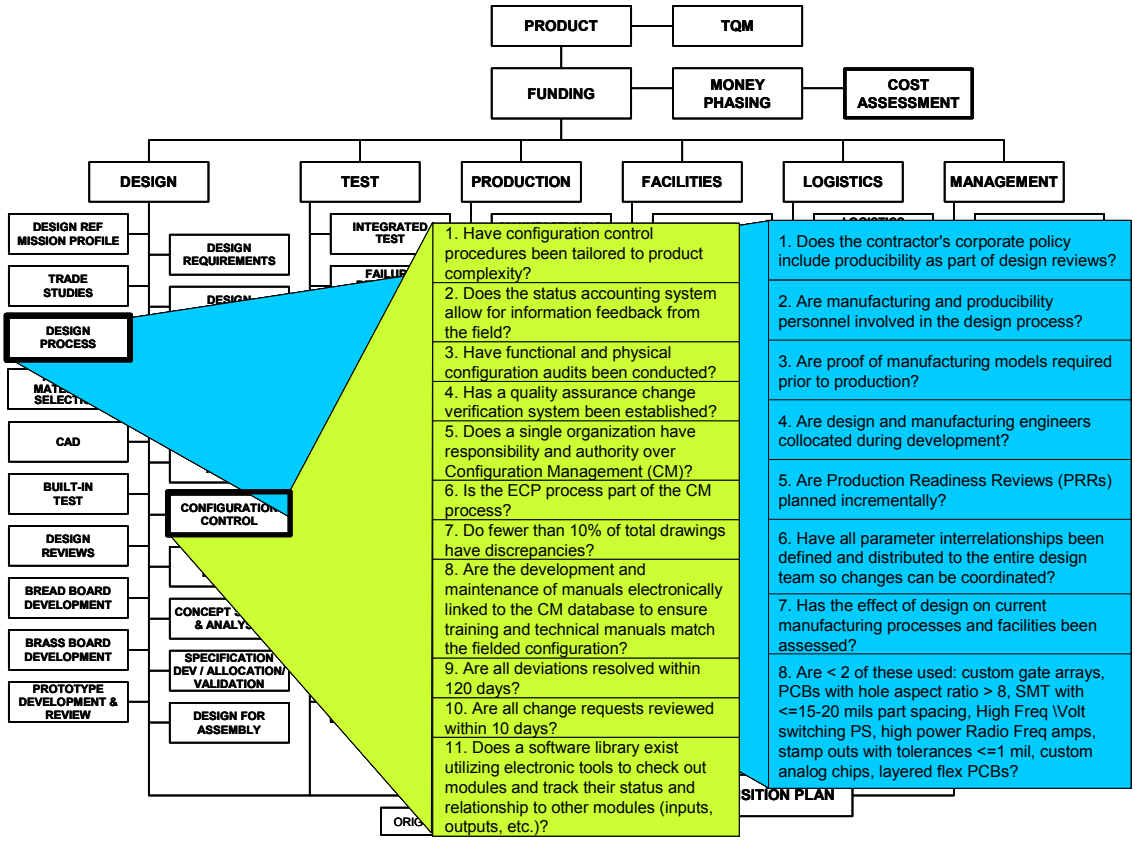


Figure 5. Sample of TRIMS Assessment Questions. From (SURTASS, 2002, p. 15)

e. Top Eleven Ways to Manage Technical Risk

In October 1998, ASN(RD&A)ABM published their most comprehensive technical risk management guidance document to date. NAVO P-3686, Top Eleven Ways to Manage Technical Risk, was created to provide the acquisition professional a single source of implementation guidance and baseline information for establishing technical risk management functions. This document contains standardized definitions, recommended methods, contractual language, training sources, critical technical processes/engineering fundamentals, best practices, software measures, and "Watch Out Fors." Although written for Navy program managers, it is also used by the other Services

and contractor program managers. NAVSO P-3686 was the first guidance document to capture many of the significant changes in the risk culture resulting from acquisition reform. It also sought to baseline some of these new methods and provide some standardization across the Navy community. Recall, ASN(RD&A)ABM's Risk Management Survey in 1997 revealed little consistency with risk management methods used by Navy program offices. There were a wide variety of risk management methods in place. The Survey results contained within this thesis indicate that NAVSO P-3686 is not quite as well known throughout the Navy community as the Willoughby Templates. Nearly 4 years after its release, a little over a third of the acquisition professionals surveyed are using this document to baseline their technical risk management programs.

NAVSO P-3686 presents three primary approaches to technical risk management and selects one recommended approach. These were the three most common approaches used within the Navy by acquisition programs as determined by the ASN(RD&A)ABM survey. Table 3 is extracted from NAVSO P-3686 and illustrates a comparison of the approaches with the recommended approach highlighted. The first approach is called the Process approach which is simply a Templates or best practices approach. The second approach is the Product approach, which assesses risk associated with systems, subsystems, and components defined by the WBS. The third and recommended approach is a combination of both the Product and Process approaches. It is called the Integrated Process/Product approach, which is consistent with the Total Program Risk Model discussed later. Table 3 summarizes the advantages and disadvantages of each.

Table 3. Comparison of Technical Risk Management Approaches. From (NAVSO P-3686, 1998, p. 6)

Approach	Advantages	Disadvantages
Process	• Proactive focus on critical processes • Encourages market search for best practices/benchmarks • Reliance on fundamental design, test, and manufacturing principles • Addresses pervasive and subtle sources of risk • Technical discipline will pay dividends in cost and schedule benefits	• Less emphasis on the product oriented elements of a program • Perception that technical issues dilute the importance of cost and schedule
Product (WBS)	• Commonly accepted approach using a logical, product oriented structure • Relates the elements of work to be accomplished to each other and to the end product • Separates a defense material item into its component parts • Allows tracking of product items down to any level of interest	• Does not typically emphasize critical design and manufacturing processes, or product cost • Risk is typically expressed as a probability estimate rather than a process variance • Delayed problem identification (reactive)
Integrated Process/ Product	• **Maximizes the advantages of Process and Product approaches**	• **None significant**

NAVSO P-3686 devotes an entire chapter (Chapter 5) to engineering fundamentals. These are defined as basic disciplined processes and practices associated with the design, test, and production functions. This sounds very much like the Willoughby Templates which in fact is the case. This chapter contains a compilation of the design, test, and production template areas with associated best practices and measures of effectiveness from earlier Navy publications. The items were updated as necessary with new best practices and lessons learned. It also expands the list of "Watch-Out-Fors" originally included in *Methods & Metrics*. A "Watch-Out-For" is defined as "requirements, conditions, materials, types of equipment or parts, and processes that almost invariably create potential or actual risk." (NAVSO P-3686, 1998, p. 19). Figure 6 illustrates an abbreviated "Watch-Out-For" list for the Design Reviews template area.

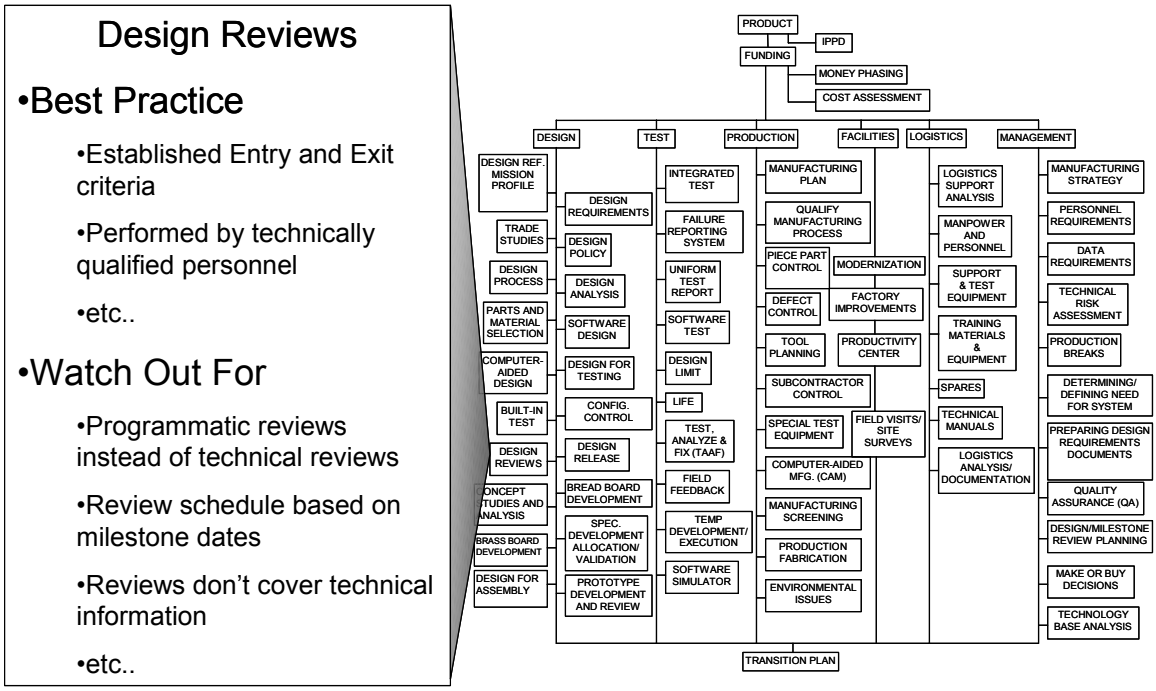


Figure 6. Design Reviews Template Abbreviated "Watch-Out-For" List.

After (NAVSO P-3686, 1998)

2. Total Program Risk

Figure 7 illustrates a Total Program Risk Model, which includes both qualitative and quantitative risk assessment methods. It comprises an Integrated Process/Product approach to technical risk assessment as recommended by NAVSO P-3686. All risk management and assessment methods used by government and industry can fit within this generic model. Risk can be categorized as either technical or non-technical. Technical risk is comprised of Process and Product risk. Process risk looks at the variance between current program practice and best practice as outlined in the Willoughby Templates. Product risk is hardware and software product related and based on expert opinion and technology maturity. The WBS is often used as a roadmap for Product risk identification. Both Process and Product risk assessments are considered qualitative approaches because the risks are determined through purely subjective assessments by the evaluators/assessors. In addition, they rely on subjective risk classifying (rating) criteria. This means there is a potential for two or more assessors to arrive at different risk levels while using the same subjective criteria. Probabilistic Risk Assessment (PRA) methods are grouped under the technical risk category and are typically product specific based on "what if" scenarios and Failure Mode Effects Analysis (FMEA).

The other major component of the Total Program Risk Model is non-technical risk. Non-technical risk can be both qualitative and quantitative. The qualitative component is simply those programmatic risks that don't qualify as a process or product (technical) risk. The quantitative components of non-technical risk consist of Cost and Schedule Risk Analysis using Monte Carlo simulation methods. Since technical risk has been defined as process-based risk that drives all other risk, the Cost and Schedule Risk Analysis methods are considered non-technical risk in this model. Recall, the qualitative technical risk component assesses the impact to cost and schedule in addition to performance. The difference lies in the fact that Monte Carlo simulation techniques are not used to quantify the risk as with Cost and Schedule Risk Analysis methods.

Ideally, both technical and non-technical qualitative and quantitative methods should be used to ensure complete risk coverage. However, most acquisition programs use either a qualitative or quantitative method, but not both. Within the Navy, qualitative

methods are used predominately. In general, the Air Force and NASA are users of quantitative methods.

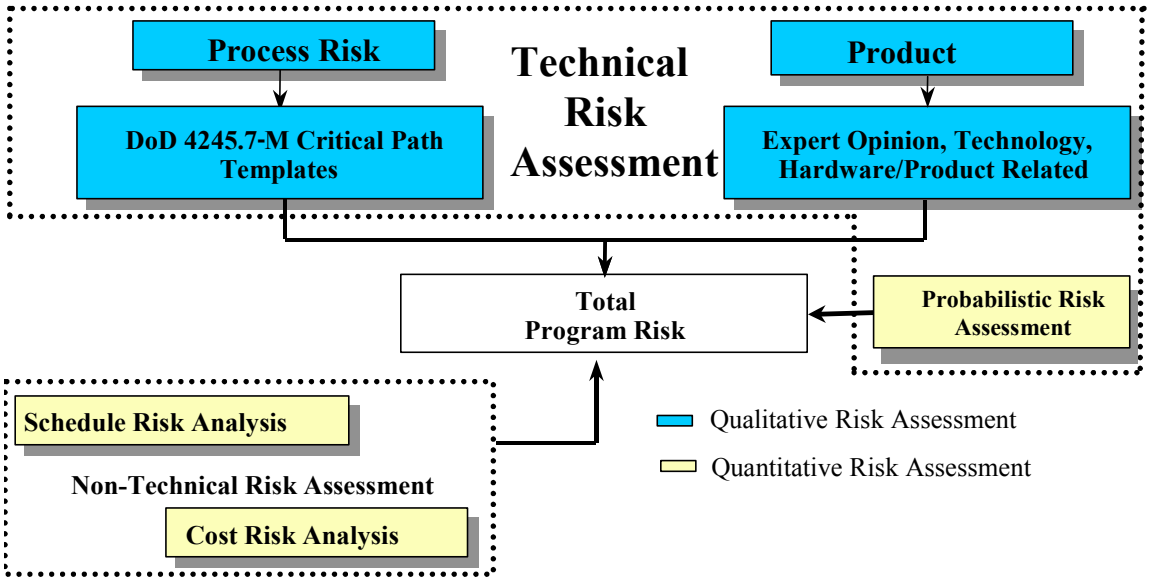


Figure 7. Total Program Risk Model

3. Risk Assessment Techniques: The Qualitative Approach

Methods & Metrics provided the first graphical representation of a process based risk assessment strategy using a qualitative approach. The methodology outlined in this guidance document was a proven process that had been in use by some acquisition professionals for nearly 10 years since the release of the Willoughby Templates in 1985. However, it remained undocumented until now. This methodology was used extensively for conducting PRRs to assess transition from development to production risk just prior to MS III. It was used by independent risk assessment teams tasked by program managers to conduct independent risk assessments on their programs, prime contractors, critical subcontractors, or key suppliers. It was a methodology of choice for contractor evaluations, such as technical assistance visits, because it provided a license to look beyond a standard contractual audit. Recall, the focus was on best practices, not simply

contractual requirements. Often, a program office would have a risk written against it for not contractually requiring of a contractor a best engineering practice. Everyone is fair game in a risk assessment, and it does not just focus on contract compliance issues. The methodology has been refined slightly since *Methods & Metrics* was released in 1994 to add product and non-technical risk paths. Figure 8 provides a look at this methodology and highlights the process based risk assessment path. Process risk assessment is the recommended starting point for any risk assessment as Process risk leads to Product risk. After Process risks have been identified, the Product and non-technical risk assessment paths should be followed.

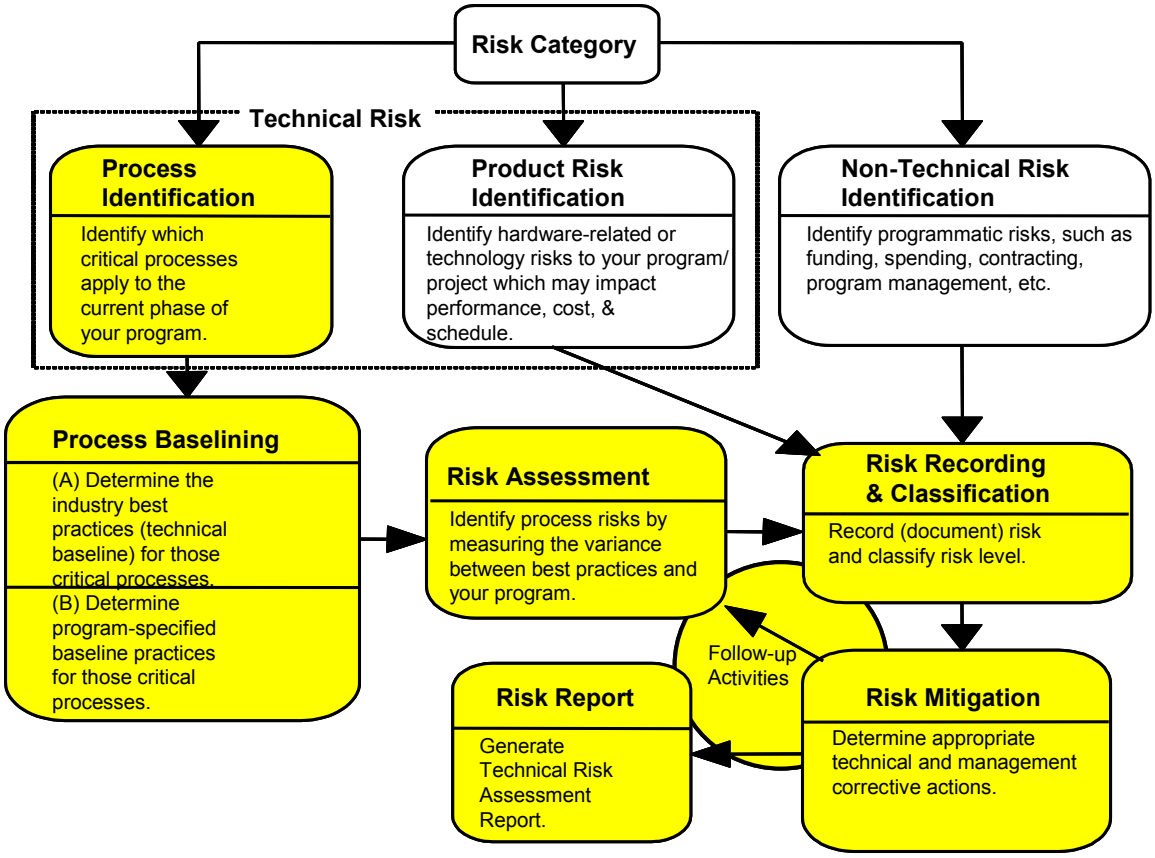


Figure 8. Qualitative Risk Assessment Model. After ("Methods & Metrics," 1994, pp. 7-16)

a. Process Identification

Process identification is the first step in a purely process-based risk assessment approach. The approach is to identify the critical engineering, manufacturing and management processes in place for the current phase of the acquisition program. Let's illustrate with an example. Let's take an acquisition program in the Engineering & Manufacturing Development (EMD) phase (System Development & Demonstration phase per the new DoD 5000 series). The prime contractor chooses to implement selected design analysis tools, including reliability prediction and Failure Modes Effects & Criticality Analysis (FMECA). Hence, we have just identified the design analysis processes used on this program.

b. Process Baselining

The second step in a purely process-based risk assessment approach is to perform process baselining. This step determines the industry best practice for program's critical processes identified in the previous step. This constitutes the technical baseline for the program's critical processes. Sources of best practice guidance information can be found in DoD 4245.7-M, NAVSO P-6071, *Methods & Metrics for Product Success*, NAVSO P-3686, and BMP's Program Manager's Workstation. Expert opinion of subject matter experts is another key source of best practice information.

Let's continue with our example. Best practice dictates a more comprehensive design analysis tool kit be used during EMD, including sneak circuit analysis and worst-case tolerance analysis. As a matter of fact, these tools should be applied during the previous phase as well. Any of the technical risk guidance documents mentioned in this thesis would recommend a more expansive application of design analysis tools to minimize risk.

Sometimes the process baseline is dictated by the customer. In this case the customer/program specifies the baseline practice for the critical process. In our example, let's assume that a thermal analysis was mandated by the customer. Hence, the technical baseline is defined by an industry best practice or by the customer or a

combination of both. This is known as program specified baseline practices for the critical processes. Typically, the customer dictates process baselines through specifications, standards, and other contractual requirements. The thermal analysis is a program-specified baseline practice specified by the customer.

c. Risk Assessment

The next step in the process is the conduct of the risk assessment. This is the act of measuring the variance between best practice (industry benchmark) and the program/project's practice. If the baseline practice is customer specified, it still must be compared to best practice, and if it does not meet best practice, a risk should be written against the customer for invoking a risky process.

The amount of variance determines the risk level. Risks are classified as High, Moderate, and Low. Risks are classified by using subjective assessment criteria, and the most common methods will be discussed in the next paragraph. In our example, the best practice guidance documents dictate additional design analysis tools, such as sneak circuit and worst-case tolerance analyses, that should be used on this program to minimize technical risk. Since these additional tools are not used on this program, there is some level of variance between standard practice and best practice. Risk classification methods are used to evaluate the level of risk.

d. Risk Recording & Classification

The next step in the technical process-based approach path is Risk Recording & Classification. This step involves documenting the risk on a Risk Identification Form (RIF) or in a risk database and classifying the risk into High, Moderate, or Low risk levels. The RIF contains all the necessary fields to adequately document and track the risk including risk mitigation plans and milestones. It also assigns ownership responsibility to an individual or IPT to ensure the risk is addressed. Most effective and productive risk management programs then transfer the RIF information into a risk database. This is needed in order to effectively and efficiently track, trend, and report the data.

Many programs automate the risk identification process to facilitate data entry. The process and database must be user friendly or people will not use it; a lesson learned from experience. A sample RIF is shown in Figure 9 and Appendix A. The appendix also includes instructions for completing each field of the RIF.

There are a number of methods available for classifying or assigning a risk level to a risk. All methods are considered qualitative, because they are subjective in nature, some more than others. The earliest methods consisted of a simple qualitative list of criteria for each risk level (Low, Moderate, and High). They were developed to support technical risk assessments conducted using the Willoughby Templates. Each Service developed their own set of narrative criteria independently because there was little guidance available. NAVSEA provided risk classification criteria in an instruction (NAVSEAINST 4800.2A), which was canceled a few years later without replacement. Within each Service, each program office used different criteria, if they conducted risk assessments at all. The three categories of risk levels remained the only common aspect concerning these narrative criteria. The lack of standardization made it difficult to assess the relative severity of risk among various acquisition programs especially among the Services.

A sample set of narrative classification criteria is shown in Figure 10. It was aptly named the "Risk Ruler" and is the culmination of 14 years of use and development by Naval Surface Warfare Center (NSWC) Corona Division and this author in support of independent risk assessments and PRRs. NSWC Corona used "Risk Ruler" extensively to assign risk levels in support of technical risk assessments on various NAVSEA and SPAWAR ACAT I and II programs. It was updated many times with lessons learned to improve the rating capabilities. It is still used today as a backup and check on the results of newer matrix based methods. It is a purely qualitative collection of subjective classification criteria.

RISK IDENTIFICATION FORM		TRACKING NUMBER XXX--XXXX--###
RISK TITLE:	**PROCESS AREA** Category: Template:	**FACILITY & PRODUCT/SUBASSEMBLY** Activity: Product:
REFERENCE	Date Identified	**DERIVED RISK LEVEL** (Low, Moderate, or High)
	ASSESSOR Name: Phone #:	**RISK LEVEL IDENTIFIERS** (Use P(f) & C(f) Tables and R(f) Matrix) **R_f:** **Probability of Occurrence (P_f):** **Consequence of Occurrence (C_f):** Performance: Schedule: Cost:
	ACTIVITY POC Name: Phone #:	
RISK DESCRIPTION & RECOMMENDATIONS:		
RISK LEVEL RATIONALE:		
ACTIVITY RESPONSE W/MITIGATION PLAN & SCHEDULE:		**RISK OWNER/IPT:** Name: Phone #: IPT:

DISCLAIMER: The Risk Assessment Team does not have the authority to direct the Contractor in any way nor alter the Contractor's contractual obligations. The Contractor shall take no action unless changes are issued in writing from the Contracting Officer. Any changes taken without official approval from the Contracting Officer shall be taken at the Contractor's own risk.

Figure 9. Sample Risk Identification Form. From (NSWC Corona, 2000)

Risk Ruler

Risk Level Standard Guidelines

Low Risk

A Low Risk is assigned when there are few differences between standard practices and best practices, but the differences are not likely to impact Performance, Schedule, or Cost. A Low Risk is considered a **normal business Risk**. Normally, plans are in place to manage the risk and personnel have past experience dealing with the risk on previous programs. Low Risks are the most common Risk category because the transition from development to production contains an inherent, unavoidable degree of Risk. The following properties characterize the Low Risk category:

- Few differences between standard and best practices.
- The Government Program Office is aware of the differences.
- Low probability of impacting Performance, Schedule or Cost.
- Normal business Risk.
- Adequate slack time to resolve the risk.
- A solution is demonstrated and plans are in place to implement a solution.

Moderate Risk

A Moderate Risk is assigned when there are some differences between standard practices and best practices. **Increased management attention** and monitoring is needed to correct the differences before they affect Performance, Schedule, or Cost. Normally, plans are in place to correct the risk, although the solution may not necessarily have been demonstrated. A Moderate Risk can also be assigned when no plans are in place, but there is adequate reserve capacity to deal with the risk. The primary difference between the Moderate and High Risk is that **management is aware** of the risk. The following properties characterize the Moderate Risk category:

- Some differences between standard and best practices.
- The Government Program Office is aware of the Risk.
- Contractor Management is Aware of the Risk.
- Some probability of impacting Performance, Schedule or Cost.
- A proposed solution exists.
- A preliminary plan is in place with an interim Schedule for implementation.
- Little slack time to resolve the risk.

High Risk

A High Risk is assigned when there are significant and substantial differences between standard practices and best practices. **Intense management attention** is needed to correct the risk before it affects Performance, Schedule, or Cost. **Management (either Contractor or Navy Management) may not be aware** of the risk and no plan exists to mitigate the Risk. A High Risk can also be assigned if plans exist but they are being inadequately implemented or there is no slack time to implement the plans before Performance, Schedule, or Cost is affected. The following properties characterize the High Risk category:

- Significant and Substantial differences exist between standard and best practices.
- The Government Program Office may not be aware of the differences.
- Contractor Management may not be aware of the differences.
- No plan or Schedule in place to implement a solution.
- Risk has High probability of impacting Performance, Schedule or Cost.
- No slack time to implement a solution.
- No work-around solution.
- Immediate High Level of management attention required.

Figure 10. Risk Ruler. From (NSWC Corona, 2000)

"Risk Ruler" was used exclusively as classification criteria for risk assessments and PRRs until matrix methods were introduced by some DoD contractors in the mid-1990s and promoted by ASN(RD&A). Now, matrix methods are taught to our acquisition workforce professionals at DAU, along with PMWS. Matrix methods were developed to provide for some consistency among evaluators when assigning risk levels. Matrix methods help to normalize risk level assignments.

One risk classification matrix method which has grown to become the most widely used method within the Navy is the 5 X 5 probability of occurrence versus consequence matrix method. Originally developed by McDonnell Douglas Aerospace for the F/A-18 program in the mid-90s, it has grown to be a standard throughout DoD ((ASN(RD&A)ABM, 1997, p. 13). There are many variants of this method also used within the Services and Industry including 3 X 3 and 10 X 10 matrices.

What led to the transformation from narrative "Risk Ruler" classification methods to matrix methods? Acquisition reform brought an emphasis on risk awareness. Programs took more risk, and needed more efficient and accurate ways of assessing risk and assigning risk levels. Risk assessments had to be more proactive by including the probability of occurrence in the rating scheme.

Risk has two components: a probability of occurrence P(f) (i.e., likelihood) and a consequence of occurrence C(f) (i.e., impact). Consequence is typically defined as having an impact on cost, schedule, and performance parameters. Prior to acquisition reform, technical risk assessments really did not look at the probability of occurrence. The focus was on consequence or impact. The "Risk Ruler" is a great example. There is little about probability of occurrence in this criteria other than the words referring to "low," "some," and "high probability." In fact these words are new perturbations added to the "Risk Ruler" somewhat recently. The problem with assigning a risk level using only the consequence parameter is that it results in an inefficient means of prioritizing risks for mitigation. For instance, a High risk may be assigned because if it occurs it could have a significant cost, schedule, or performance impact on the program. Because it is assigned a High risk, it would be a top priority item for

mitigation. However, in actuality the probability of occurrence may be very low, so the risk should have been assigned a low priority for mitigation. This failure to include a likelihood of the risk occurring was not such an issue prior to acquisition reform when defense budgets were large. Most of the risks could be addressed because resources were available. After the end of the Cold War and the start of declining defense budgets, most programs had limited resources available for mitigation actions, and had to prioritize risks more accurately, necessitating the addition of a probability of occurrence factor to the classification formula. No longer could programs mitigate every risk. In addition, risks were being identified much earlier to affect a more proactive approach. The earlier risks are identified the cheaper it is to manage and reduce the risk.

Matrix methods also provide an added bonus of reducing subjectivity. The matrix method is a little more quantitative because it assigns a rating value (whole number) to the probability of occurrence and consequence. It is still considered qualitative because the assignment of whole number ratings is based on subjective criteria contained in the probability of occurrence and consequence tables. Because traditional narrative criteria is transformed into a whole number rating, this in effect normalizes the risk rating (classification) process. With a purely subjective risk classifying approach, there is the potential for assessors to arrive at different risk level ratings while using the same criteria, such as the "Risk Ruler." For both these reasons of more efficient prioritization and reduction in subjectivity, the Services and their contractors are using 5 X 5 or equivalent P(f) vs. C(f) matrices to classify risk. ASN(RD&A)ABM's 1997 Risk Management Survey confirms this fact that of the 41 Navy acquisition programs surveyed, the predominant risk classification method used was the P(f) vs. C(f) matrix method ((ASN(RD&A)ABM, 1997, p. 6). This method is used to classify risk for all categories of risk: technical, non-technical, and programmatic. A typical 5 X 5 risk classification matrix is shown in Figure 11. Variants of the 5 X 5 Matrix Method are shown in Appendix B.

Probability of Occurrence (IF)		
Level	**Probability** (Product / Process)	**Definition** (Product Risk)
1	Unlikely / Using Existing and Proven Industrial Best Practice	Extremely Rare. Current Actions OK. *Easily and Quickly* resolved.
2	Some Chance	Low Likelihood. Current strategy *should* resolve this issue.
3	Even Shot / Newly Developed and Proven Process or Not Industrial Best Practice	Likely to occur. Current strategy *may or may not* resolve this issue. Work-arounds may be required.
4	Good Chance	Highly Likely. Current strategy *will probably fail* to resolve issue. Alternative plans will be required.
5	Very Good Chance / Using Unproven and Newly Developed Process.	Near Certainty. Current strategy will not resolve this issue. Alternatives will be required or intense (management) attention.

Consequence of Occurrence (THEN) Assume Event Has Occurred (For Overall Risk Level Classification use Highest Level among consequence parameters.)			
Level	**Technical/Performance**	**Schedule**	**Cost**
1	Minimal/No Impact	Minimal/No Impact	Minimal/No Impact
2	Small Reduction No Work-Arounds Needed	Minor Slip (Won't Affect Critical Path)	Small Reduction in Contractor/Activity's Management Reserve (MR) Margin
3	Moderate Reduction Work-arounds available	Moderate Slip (May Affect Critical Path)	Significant Reduction In Contractor/Activity's MR Margin
4	Significant Reduction Possible Alternatives	Significant Slip (Will Affect Critical Path)	Contractor/Activity Overruns MR
5	Cannot Achieve Tech. Performance No Alternatives	Major Milestone Affected	Contractor/Activity Requests More Funding

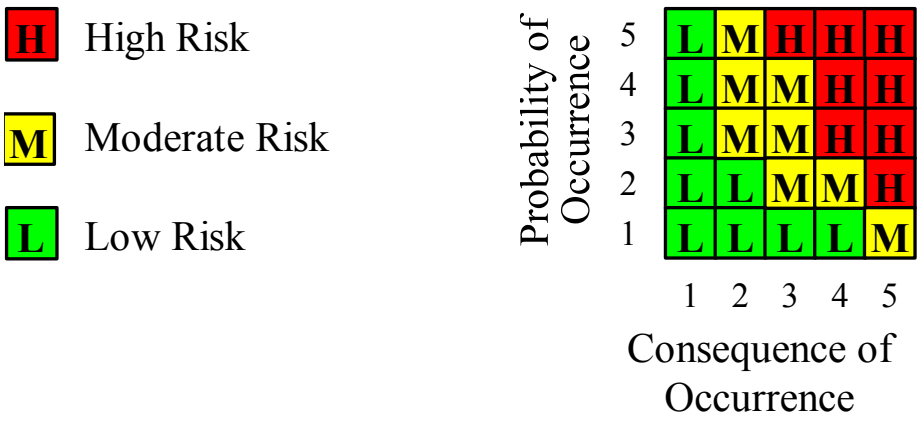


Figure 11. 5 X 5 Risk Matrix. From (NSWC Corona, 2000)

Risk is defined as the uncertainty of attaining a future goal. The key is "a future goal," not a current event or an event that has already occurred. If it is a current event or an event that has already occurred, then it is a problem, not a risk. If it is a sure thing (100% probability), then it is a problem, not a risk. A risk is a future event which might occur if risk mitigation actions are not taken. Too often risks do not get sufficient management attention until they result in problems. By this time it is too late and corrective actions almost always cost more and take longer.

Risk is quantified by assessing the intersection of probability and consequence. The probability of occurrence table looks at how likely it is the risk event will occur on a scale from 1 to 5, where 1 is unlikely to occur and 5 is a very good chance that it will occur (almost certainty or 100% probability). The definitions in the Probability Column apply nicely to Process risk. The definitions in the Definitions Column apply nicely to Product risk, as well as non-technical and programmatic risk. Table definitions may be tailored by program/project.

The consequence of occurrence table looks at the severity or impact the risk event may have on cost, schedule, and performance assuming the event has occurred. A whole number value in the range of 1 to 5 must be assigned to each consequence parameter (i.e., cost, schedule, and performance). Each whole number value for performance, schedule, and cost must be annotated on the RIF. The highest rating for all three consequence parameters is used to obtain the overall risk level or risk factor and is also annotated on the RIF. The assumption is that each consequence parameter (i.e., cost, schedule, and performance) is equally weighted. Unless otherwise stated in the C(f) table definitions, the criteria can be applied to the process, product (hardware/software), and program levels. This is why the criteria are written in a generic fashion. Table definitions/criteria may be tailored by program/project.

The Resultant Risk Level R(f), also known as Derived or Cumulative Risk Level or Risk Factor, is determined using the cube in Figure 11. The Resultant Risk Level is the intersection of the Probability of Occurrence P(f) value and the largest of the Consequence of Occurrence C(f) values for cost, schedule, and performance. It provides

for the calculation of an overall risk level based on whole number ratings. This R(f) cube can also be tailored depending on how lenient or conservative you want to be. For instance, some programs change cell (3,4) from "H" (High) to "M" (Moderate).

Why use a 1 to 5 scale? This appears to be an optimum scale for trying to quantify a subjective process, which is substantiated by this author's experience in using this scale. Some programs use a 3 X 3 matrix. This does not provide for enough dispersion. Some programs use a 10 X 10 matrix. This provides too many choices and slows down the classification process. It is also more difficult to use by the assessor and provides for too many choices, hence it is difficult to obtain any sort of repeatability or consistency among assessors. The 5 X 5 Matrix Method is highly recommended by this author because it is simple and easy to use with short and succinct classification criteria and is also tailorable by program/project.

"Risk Ruler" can be used alone or in conjunction with the 5 X 5 Matrix Method. The author recommends that the "Risk Ruler" be used in conjunction with the 5 X 5 Matrix Method to validate the results. Words/verbiage from the "Risk Ruler" should be used to fill in the "Risk Level Rationale" field of the RIF. "Risk Ruler" should be used to adjudicate disagreements on risk level assignments among assessors/ evaluators.

Documenting the risk is an important task that must be given due diligence. Roughly 80% of the complete risk assessment and management effort is attributed to data collection and documentation. It takes time, but it must be done right. The RIF shown in Figure 9 and Appendix A is one method of collecting risk information. Detailed definitions for each field are also provided in Appendix A. Many programs today use automated risk databases to identify, collect, track, and report risk information. Regardless of the method of data collection, there are some recommended fields of risk data that should be collected as shown in Figure 9 and are described below.

The "Process Area" field of the RIF is where the process area under review is annotated. For those using the Willoughby Templates as an assessment baseline, the Willoughby Template category is referenced in the field along with the

applicable template area. For example, if a risk was written against a contractor's Configuration Control process, the individual filling out the RIF would put "Design" in the Category block and "Configuration Control" in the Template block. If more than one template applies to the risk, the most applicable one is chosen. This will make the reporting process by template much easier.

The "Risk Level Identifiers" field is where the assessor's ratings for P(f) and C(f) are documented (if this method is used). If the "Risk Ruler" is used instead, then the risk level rationale from the "Risk Ruler" is written in the "Risk Level Rationale" field of the RIF. Some risk management programs use both the probability and consequence matrix method and "Risk Ruler" approaches to arrive at an overall (derived) risk level. If the matrix method approach is used, the "Risk Level Rationale" field is used to explain why certain P(f) and C(f) rating numbers were selected. The "Derived Risk Level" field is where the overall risk rating is documented resulting from the classification method chosen.

The RIF has a "Risk Owner/IPT" field and a "Contractor Response with Mitigation Plan & Schedule" field. Thus, the RIF provides for complete closed-loop traceability from risk ownership to mitigation planning and scheduling. Risk mitigation plans and schedules may be attached as separate documentation to the RIF when additional space is required. RIFs should be placed in a risk management database for tracking, trend analysis, and reporting. Appendix C provides a sample risk write-up.

Continuing with the flow of the top-level Qualitative Risk Assessment Model in Figure 8, Risk Recording & Classification is where the path converges with the other qualitative approaches, such as Product & Non-technical. From this point on the same steps apply to all qualitative and quantitative approaches. These common steps are Risk Recording & Classification, Risk Mitigation, Risk Reporting, and Follow-up Activities. These remaining steps have to be taken regardless of the risk assessment approach.

e. Risk Mitigation

The next step in the process-based approach path is Risk Mitigation -- what to do with the risk once it is identified and classified. As mentioned previously, this step is not unique to a qualitative technical risk management approach. It also applies to any of the qualitative and quantitative methods. Risk mitigation consists of planning and executing tasks to reduce the identified risk to an acceptable level. After the assessor documents the risk and assigns a risk level with rationale, the contractor (or government activity) typically completes a POA&M or mitigation plan for reducing the risk. The Contractor/Activity must complete the activity response field of the RIF. The mitigation plan must be summarized in the "Activity Response With Mitigation Plan/Schedule" field of the RIF or attached as a separate document to the RIF. In today's IPT environment the mitigation plan is often drafted by an IPT, which includes customer representation. This field must list mitigation plans with key events and milestones. This is necessary in order to feed back this information into the WBS/Integrated Master Schedule (IMS) planning packages so the mitigation plans get incorporated as program work elements. This ensures the work gets done and that resources are allocated to implement the mitigation plans.

The assessor often provides risk mitigation recommendations as part of the "Risk Description" on the RIF. This is valuable because it gives the responsible activity a place to start with risk mitigation actions. Remember, risk assessment teams are comprised of subject matter experts, and their advice and recommendations should be heeded.

The assessor is cautioned, however, not to give or appear to give contractual direction. The assessor is not authorized to do so. Any actions taken by the Contractor/Activity on recommendations made by assessors shall be taken at the Contractor/Activity's own risk or within the constraints of the contract. A disclaimer to that effect should be placed on the RIF and made perfectly clear to the activity under review before, during, and at the end of the risk assessment.

Mitigation plans are typically only written for Moderate and High risks. This is why risks are classified into three levels (L, M, H), so limited resources can be allocated to the most significant areas for mitigation. Low risks should still be monitored to make sure the risk levels do not escalate. Some programs write mitigation plans for Low risks in addition to High and Moderate risks. Mitigation plans and schedules must also be included in the risk management database if used. It is highly recommended that a risk management database be used to ease the tracking of risk mitigation plans and actions.

f. Risk Reporting

The next step is to report risk status which is done periodically to management and the customer. Risks and risk mitigation status are followed up on and reassessed until closed or reduced to acceptable levels. Risk reporting consists of two levels. The first level of reporting is comprised of risk assessment team reports resulting from on-site risk assessments. A typical outline for a technical risk assessment report after an on-site risk assessment of a contractor/activity/program by a risk assessment team is as follows:

- Executive Summary
- Functional Area Summaries (Management/Funding/Transition Planning, Production/Facilities/Logistics, and Design & Test)
- Red, Yellow, Green Quick Look Risk Template Summary Chart
- Risk Identification Forms for all risks
- Risk mitigation recommendations
- Risk mitigation planning, milestones, and corrective actions
- Risk identification, classification, and mitigation trend analysis
- Waterfall Charts showing risk mitigation progress over time

Functional area summaries are generally written by technical risk assessment team leaders to summarize what their team found. Typical risk assessment (functional area) teams are:

- Program Management
- Reliability/Design
- Test & Evaluation
- Production/Facilities/Logistics

The next level of reporting is a higher level of reporting for management. It consists of a stop light presentation of program risks. Figure 12 shows an example of this type of risk report for a technical risk assessment conducted per the Willoughby Templates. This quick look red, yellow, green template report shows in graphical, color-coded format what the risk levels are per template area for the project/program being reviewed. It can also be applied at the subcontractor and supplier levels. Additional templates or review areas can also be added to this template tree.

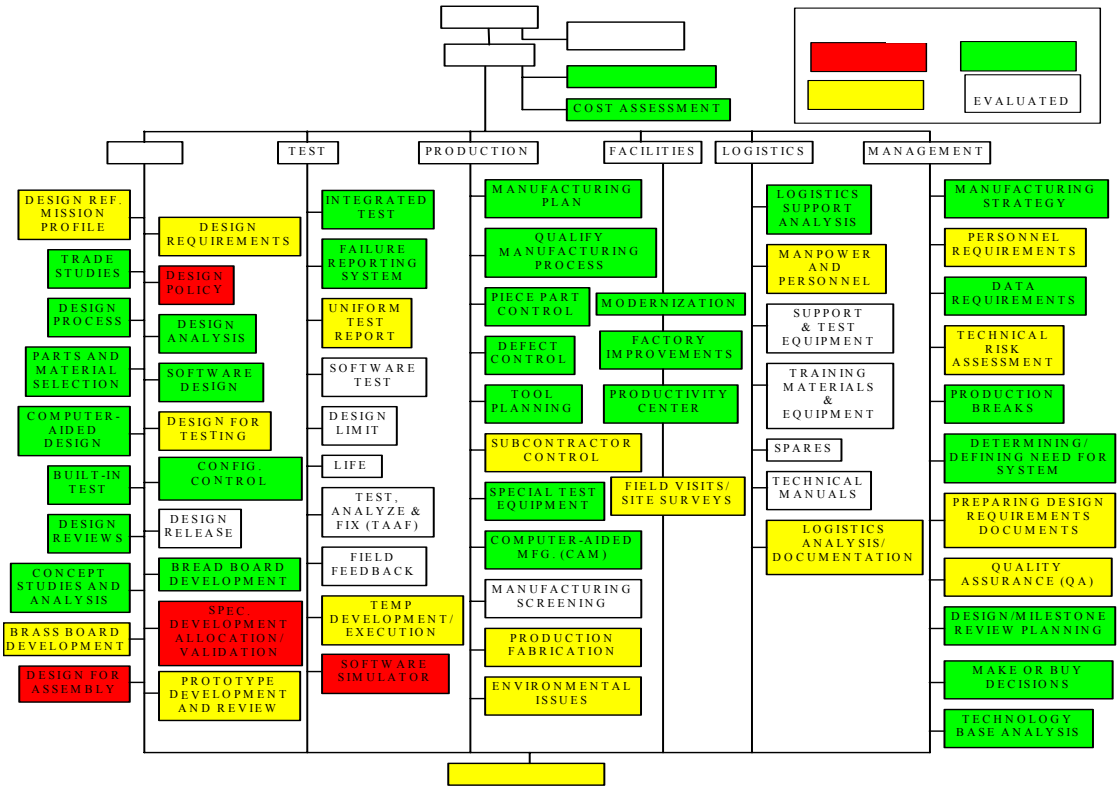


Figure 12. Sample Quick Look Reporting Format. From (NSWC Corona, 2000)

How are risk levels rolled up? Each template contains a number of control methods as outlined in the Willoughby Templates (DoD 4245.7-M) or stated as questions in the TRIMS database. The highest risk assigned to a control method or question within a template area becomes the risk level assigned to the entire template. In other words, if there are 10 control methods or questions under the Design Policy Template and one of the 10 control methods/questions is a High risk, 3 of 10 are a Moderate Risk, 5 are a Low risk, and one is Not Applicable, then the Template is assigned an overall risk level of High or Red. The worst-case risk level drives the overall risk level for the Template. In a similar manner the worst case Template drives the rolled up risk level at the Template Category level (i.e., Design, Test, Production, Facilities, Logistics, Management). TRIMS does not use a worst-case method, but instead uses a tailorable weighting scheme that renders certain assessment questions more important than others. Appendix D provides samples of additional reporting methods.

g. Follow-up Activities

This is the final critical step in both a qualitative and quantitative risk assessment process and is the key to effective risk mitigation or corrective action. This is done through periodic re-assessment of risks and verification of risk mitigation actions. Constant feedback will ensure that program/project risks are known and are being managed appropriately.

A common mistake is not following-up on Low risks or closed risks. Many Low risks, if not periodically monitored, could escalate into higher level risks, transforming themselves from a benign issue or normal business practice into something more serious impacting one or more cost, schedule, and performance parameters.

Another common mistake is not periodically following-up on closed or accepted risks. Accepted risks are those risks normally closed at a higher risk level with rationale stating that nothing can be done to mitigate the issue. Thus, they must be accepted by the program/project. Closed and accepted risks must be periodically re-addressed to ensure that the risk issue has not been re-opened due to new developments

or current actions. Accepted risks bear watching for potential risk mitigation solutions that may surface over time. A good example is a sole-source supplier of a critical hardware item. This is a program risk, and at the time the risk was written there were no other suppliers in the world capable of producing the same item. Now, a few years later there are a couple of alternate suppliers available. This risk may be re-opened and risk mitigation measures taken to try and qualify one of the new suppliers as an alternate source. Keep in mind that a change in one risk's risk level can affect another risk's risk level. Insight into risk mitigation efforts is the key. Insight is gathered through thorough risk assessment follow-up activities.

4. Risk Assessment Techniques: The Quantitative Approach

A risk awareness culture was brought about by acquisition reform. Programs are taking more risk and thus accepting more risk. The goal of the systems engineering process is to balance cost, schedule, performance, and risk. Our product development models encourage risk taking. Program managers are told there are no opportunities without risk. Risk management has been elevated to a key component of project management. With the greater emphasis on risk identification and mitigation there has emerged a need for more quantitative risk assessment methods. A purely subjective assessment of risk level is not always adequate to assess the probability of occurrence and impact on a mission critical event, such as an O-ring failure on a solid rocket booster. Often more insight is needed which qualitative methods cannot provide. Wouldn't it be nice to model in probabilistic terms how likely it is that an O-ring might fail on the shuttle during launch for a certain temperature range? Wouldn't it also be nice to know what the impact would be if the risk event occurs? For the solid rocket booster O-ring an example of a quantitative impact might be loss of a certain percentage of thrust, loss of right or left booster, or in the worst case scenario loss of vehicle and the crew. Qualitative methods would only provide a Low, Moderate, or High risk of O-ring failure resulting in loss of vehicle.

Decision makers are faced daily with critical decisions that can impact cost, schedule, performance, and safety. Thus, they desire as much insight as possible into their programs and that includes risk.

Over the past decade, quantitative risk assessment methods and techniques have grown considerably within government and industry. NASA has been a forerunner in the development, acceptance, and use of one of the more popular quantitative methods called Probabilistic Risk Assessment (PRA). This driving force by NASA all started after the Challenger disaster. (NASA, 2000, p. 1)

PRA is a quantitative probabilistic modeling process that uses a variety of logical analysis tools, such as FMEA and fault tree analysis, to identify risk scenarios and quantify risk. As with qualitative methods, PRA is comprised of two components, the probability of occurrence and consequence of occurrence. The difference lies in how the risk is classified. Qualitative methods use subjective assessments, such as Low, Moderate, and High. Quantitative PRA methods assign a probability or frequency number to the likelihood of occurrence. The consequence component is also assigned a numerical value (i.e., number of individuals potentially killed). (Stamatelatos, 2000, p. 1)

PRA originated in the early 1960s in the aerospace industry and missile programs. The Apollo program shunned PRA when an analysis revealed a very low probability of success of landing a man on the moon. Instead, NASA focused on engineering discipline and process rigor. As Stamatelatos (2000, ¶ 4) aptly phrased it, "NASA decided to rely on the Failure Modes and Effects Analysis (FMEA) method for system safety assessments…FMEA continues to be required by NASA in all its safety related projects."

While NASA ignored PRA methods, the nuclear industry started using these methods to conduct safety studies. Sandia National Laboratories developed PRA methods to conduct safety studies of nuclear weapons, and expanded to include studies of nuclear reactor safety in the 1970s. PRA results were used to justify the safety and continued existence of nuclear power reactors for electricity generation. (Sandia, n.d., ¶ 1)

Over the course of 20 years from the 1960s to the 1980s, PRA methods were refined, improved, and expanded to other industries including petroleum, chemical, and environmental industries. By the time of the Challenger accident, PRA methods had repeatedly proven their ability to uncover design and operational weaknesses that many experts could not find using conventional methods. One output of the Challenger investigation was a recommendation that PRA methods be used by NASA to estimate the probability of failure of critical shuttle components. Since this time, PRA methods have been used as an important risk assessment and decision support tool.

Within the last few years NASA has undertaken a corporate effort to expand their in-house capabilities in PRA. They are training people to increase awareness and use of PRA. Recent directives have been released which mandate the use of PRA on high profile and mission critical systems. NASA just released in August 2002 a *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. It can be downloaded from the following site: http://www.hq.nasa.gov/office/codeq/risk/risk.htm. (NASA, 2000, pp. 1-5)

PRA methods are expected to grow in both government and commercial industries. (Stamatelatos, 2000, p. 3) Recently, the nuclear regulatory commission and the environmental protection agency have started using PRA methods.

The use of PRA methods in the Navy for technical risk management is not common. Although the predominate method used is the qualitative approach, NAVAIR appears to have small pockets of PRA use.

NASA is a clear leader in the PRA field. If history does indeed repeat itself, it is highly likely that PRA methods within NASA will rub off on the military services. It has happened before with risk avoidance methods and process rigor.

Our Total Program Risk Model, Figure 7, discussed previously illustrates two additional quantitative risk assessment methods that are non-technical. These methods are Cost and Schedule Risk Analysis and can be applied individually or in an integrated fashion on the Integrated Master Schedule. These methods provide for a probability estimation of how likely the program will meet cost and schedule targets. The Schedule

Risk Analysis is conducted on the project schedule using a Monte Carlo simulation add-in to MS Project or equivalent Critical Path Method (CPM) scheduling tool. The risk analysis assesses the uncertainty in the specified activity duration in the project schedule. A typical CPM scheduling tool assumes that the activity durations are known with certainty, which is not the case. The scheduling software rolls up these durations to a project completion date. Because of the inherent uncertainty in the activity durations, this completion date is not realistic. A Schedule Risk Analysis takes into account the uncertainty in the durations by representing the uncertainty as a 3-point triangular distribution made up of 3-point estimates. These 3-point estimates are the most likely, pessimistic, and optimistic durations. The most likely activity duration is what is originally loaded into the schedule. Cost account managers are interviewed by risk assessors to determine the worst case (pessimistic) and best case (optimistic) durations for each activity in the schedule.

A similar methodology is used to conduct a Cost Risk Analysis, and the best case and worst case costs are also considered in addition to the most likely value. This data collection process is the most time consuming part of a Cost & Schedule Risk Analysis and accounts for approximately 80 to 90% of the effort. Once the data is loaded, a simple Monte Carlo simulation tool is used which randomly selects values from the 3-point distribution and calculates total program costs and completion dates. After many iterations (approximately 3000) of the simulation tool, the results converge on final values. These results provide the most likely project end dates and costs which are not what the project scheduling tool indicated for Estimates at Completion (EAC). Hence, there is some amount of cost and schedule risk associated with the EAC. The risk is quantified in terms of a probability or percentage of exceeding costs and schedule. For example, the simulation might output a 50% probability that the project will not meet its estimated completion date. From here, the probabilities can be partitioned into levels of risk (i.e., Low, Moderate, High). (Hulett & Campbell, 2002, pp. 1-3)

Monte Carlo simulation is based on several principles of probability and on the techniques of probability transformation. One underlying principle is the law of large numbers, which states that the larger the sample the more certainly the sample mean will

be a good estimate of the population mean. Monte Carlo simulation randomly generates values for uncertain variables repeatedly until a probability distribution is converged upon. The more iterations that are applied in the Monte Carlo simulation, the smoother the probability distribution curve for project cost and schedule and the more accurate the results will be. ("What is Monte Carlo," n.d.)

There are a number of commercially available software tools which perform Cost and Schedule Risk Analysis. Most of these tools are add-ons for existing spreadsheet and project scheduling tools. Crystal Ball is a Monte Carlo simulation add-on for Microsoft Excel, which can be used to perform a Cost Risk Analysis. It is available from http://www.decisioneering.com. Risk Plus and @Risk are add-ons for Microsoft Project and perform Monte Carlo simulations for Schedule Risk Analysis. The more integrated approach uses Monte Carlo for Primavera which takes the input data from Primavera's P3 project scheduling program and computes the Cost and Schedule Risk Analysis in the same simulation (Hulett & Campbell, 2002, pp. 13).

E. SOFTWARE RISK MANAGEMENT

It is imperative that software development practices follow a disciplined process similar to those associated with hardware development. There must be no difference in amount of process rigor applied. The reliance of today's complex systems on computer programs and firmware continues to grow. Over the past 20 years software development has evolved into a complete software engineering approach. Software has become a driving force in virtually every product that touches our lives. Our complex weapon systems depend tremendously on fault free and accurate software products, which require a disciplined engineering approach. The risk of haphazard development is too great. Software engineering is a subset of the systems engineering process. It encompasses processes, methods, metrics, programs, documents, tools, and data. Software engineering is a process, and software is a product (i.e., it provides information).

Because software engineering is a disciplined process, a process-based technical risk assessment strategy is necessary to measure how well software engineering

disciplines have been implemented. The process-based technical risk assessment must be conducted early in development and continue throughout the coding, testing, and maintenance phases. Ineffective process-based risk assessment on the software engineering process will lead to software product risk. Again, our tenet of Process risk leads to Product risk is applicable. (Pressman, 2001, pp. xxv, 2-3)

The Willoughby Templates, NAVSO P-6071, TRIMS, *Methods & Metrics*, and NAVSO P-3686 provide guidance and best practices for software design and test. *Methods & Metrics* provides some quantitative measures of effectiveness for software design and test. NAVSO P-3686 provides an extensive list of qualitative and quantitative software measures.

Industry uses a number of similar measures to assess software risk. The use of checklists and lessons learned are prevalent in the literature. Many of these are similar to the key questions asked within NAVSO P-6071 and the TRIMS database. Industry has also adopted the probability vs. impact methods from the Services and utilizes similar probability and impact rating tables. They generally classify risk by risk component (i.e., cost, schedule, performance, support, etc.) and role up each to an overall risk level by calculating a Risk Exposure (RE) number for each event: RE = P x C, where P = probability of occurrence and C = consequence of occurrence. Another method is very similar to a standard military Failure Modes Effects & Criticality Analysis (FMECA). Risks are rank ordered according to an evaluation of criticality (i.e., catastrophic, critical, marginal, negligible). (Pressman, 2001, pp. 146-154)

With the increasing emphasis on process maturity and discipline resulting from the software engineering process, the Software Engineering Institute (SEI) developed a model of software engineering capabilities that should be in place within a software development organization for different maturity levels. This Capability Maturity Model for Software (SW-CMM) defines key activities that must be in place at different levels of maturity to lower the risk during software development. The software CMM has five levels of maturity with Key Process Areas (KPA) defined within each level. Each process area is defined by a set of key practices, which must be in place for the KPA to be implemented. (Pressman, 2001, pp. 24-26)

Because CMM is process based it is not unlike the best practice methodology contained in the Navy templates approach. In fact, DoD has adopted the CMM methodology to conduct CMM assessments on prime contractors, subcontractors, suppliers, and other key software developers. CMM is a proactive technical risk management strategy because it promotes the application of best practices during the software engineering process. The five SW-CMM Levels are summarized in Table 4 below. Each level is an accumulation of all the lower levels (except Level 1):

Table 4. Software Capability Maturity Matrix Levels. After (CMU/SEI-96-TR-023, p. 3)

1) Initial	The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.
2) Repeatable	Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
3) Defined	The software processes for both management and engineering activities are documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
4) Managed	Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
5) Optimizing	Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

SEI has published additional CMMs related to software development including a Software Acquisition Capability Maturity Model (SA-CMM) and a People Capability Maturity Model (P-CMM). SA-CMM contains a collection of key practices to improve the software acquisition process. P-CMM extends the organizational and management aspects of the software CMM to include best practices for the management of people to support the software development and maintenance efforts. Acquisition risk management

is a KPA for the SA-CMM. CMU/SEI-97-HB-002 provides guidelines for implementing a software acquisition risk management program to meet the requirements of the acquisition risk management KPA of the SA-CMM. This is a purely qualitative, best practices approach.

The software CMM Level process areas are given in greater detail below. They are a summary of KPAs from the three software related maturity models mentioned above (i.e., SW-CMM, SA-CMM, and P-CMM). (CMU/SEI-97-HB-002, CMU/SEI-96-TR-023, CMU/SEI-95-MM-02)

Level 1: Initial KPAs: There are none at this level.

- Reactionary, on the fly responses to major problems. Minimal business experience and understanding of existing processes/products.
- Ad-hoc - chaotic.
- Depends on individual efforts.

Level 2: Repeatable KPAs:

- Staff commitments to perform individual responsibilities. Company commitment to environment, resources, information, well-defined procedures and compensation, and minimal distraction.
- Requirements Management (RM): Well established company/customer communications.
- Software Project Planning (PP): Clearly defined SE process plan.
- Software Project Tracking and Oversight (PT): Progress metrics which identify plan deviation rapidly.
- Software Subcontract Management (SM): Evaluation metrics/management for subcontractors.
- Software Quality Assurance (QA): Management and oversight of all phases for quality.
- Software Configuration Management (CM): Integrity checking/ establishment.

Level 3: Defined KPAs:

- Staff level of competency, skill, knowledge and participation. Company response to these attributes - recognition, reward. Build company profiles of human resources - commitment.
- Organization Process Focus (PF): Improve overall SE process capability.
- Organization Process Definition (PD): Determine core competency within organization. Develop long term plans for continuous process improvement.
- Training Program (TP): Develop the skills and knowledge of employees continuously.
- Integrated Software Management (IM): Integrate and continuously enhance communication channels between Software Engineers and Management.
- Software Product Engineering (PE): Continuous process/product improvement through well-defined engineering process for effective, efficient software products.
- Inter-group Coordination (IC): Establish effective communication methodologies between all SE groups to review/define customer requirements.
- Peer Reviews (PR): Peer oversight of all work products for early defect detection.

Level 4: Quantitative or Managed KPAs:

- Development of Mentoring program to encourage the reflection of excellence exhibited by certain key individuals to guide human resource management.
- Quantitative Process Management (QP): Detailed metrics/control of process and quality.
- Software Quality Management (QM): Use of these metrics to reach specific goals.

Level 5: Optimizing KPAs:

- Personal Competency Development: Piloting innovative ideas and technologies.
- Defect Prevention (DP): Perform root cause analysis of problems to adequately address them.
- Technology Change Management (TM): Identify areas that can be benefited by newer technologies and implement the changes seamlessly.

- Process Change Management (PC): Integrated product/process improvement.

Although the software capability maturity models discussed above provide a good checklist of critical software best practices and key performance areas, there is no guarantee that a software developer/vendor being certified to a particular CMM level will apply those disciplines to your program.

The software engineering process consists of seven phases of software development: Requirements, Specification, Design, Implementation, Integration, Maintenance, and Retirement. There is a direct correspondence between the cost to repair the software product and the associated risks to system stability with each phase transition in the software development. The most critical phases are the Requirements Phase, the first step in the process, and the Specification Phase, the second step. For the software developer, the time and subsequent cost, and for the program office, the risk associated with errors or omissions in these phases over the life cycle of the software can be the "Achilles heel" of the development effort. Major changes required during the Integration or Maintenance Phases due to ambiguous, implied, or undocumented system software requirements presents significant risk to the program office and instability to the software contractor. Other hazards presented are related to requirements which are too narrowly focused and scope creep (additional functionality requested after the requirements have been defined).

Software functionality must be directly mapped to the system requirements using a Requirements Traceability Matrix during the Specification Phase to reduce the risk of requirements omission. Figure 13 shows the relative cost to repair software defects if found during the first six phases.

As shown in CMU/SEI-97-HB-002, *Software Acquisition Risk Management Key Process Area (KPA) -- A Guidebook Version 1.0*, the SEI risk management strategy defines a systematic process for managing software acquisition risks. The process consists of a number of functions that are performed as continuous activities throughout a software project's life cycle. Figure 14 is a graphical depiction of these functions.

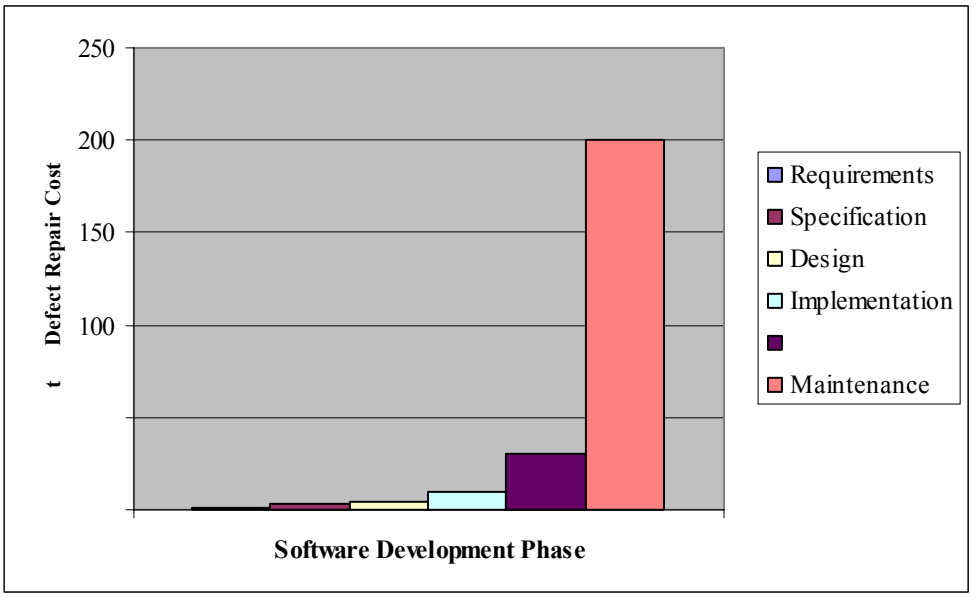


Figure 13. Relative Defect Repair Cost. From (Schach, 1999, p. 14)

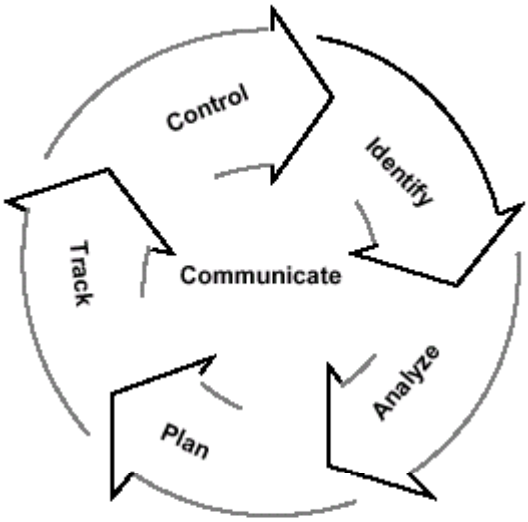


Figure 14. SEI Risk Management Process. From (CMU/SEI-97-HB-002, p. 4)

Communication and documentation are the keys to reducing the risks associated with software acquisition and development. The communication ensures that the program office adequately defines the requirements of the system, and the documentation creates a living record of the interactions between the program and developer.

Software engineering is a process and like any process its performance can and should be measured. Technical Performance Measures (TPM) are critical elements of the software engineering process. These performance measures link well to the risk management process and provide another measure of software risk. For instance, if a software performance measure is showing an adverse trend, then it is a good candidate for a risk write-up. The same holds true for program level TPMs. They should be watched and any adverse trends should warrant the generation of a risk write-up. Pressman (2001) lists some typical software TPMs used in government and industry:

- Quality Factors
- Function Points (based on inputs, outputs, inquiries, master files, and interfaces)
- Lines of Code
- Complexity
- Design structure quality index
- Cohesion and Coupling
- Interface design
- Program length and volume
- Software maturity index

In the 1990s the Object Oriented (OO) software engineering methodology has exploded in the commercial world and is quickly replacing conventional structural software engineering methods. Software developers are attracted to OO methods because they create libraries of reusable classes, objects, and components. This accelerates the

software development cycle and leads to higher quality software. The OO paradigm is also attractive to DoD software acquisitions because of it modularity and ease of upgrade. Software developed with OO techniques "is easier to maintain because its structure is inherently decoupled." (Pressman, 2001, pp. 542)

As with conventional software engineering practices OO methods must have performance measures as well. NASA's Software Assurance Technology Center has developed nine metrics for objected oriented design and development. Rosenberg and Hyatt (1997) define the following metrics in detail, which is beyond the scope of this thesis:

- Cyclomatic complexity
- Size
- Comment percentage
- Weighted Methods per Class (WMC)
- Response for a Class (RFC)
- Lack of Cohesion of Methods (LCOM)
- Coupling Between Object Classes (CBO)
- Depth of Inheritance Tree (DIT)
- Number of Children (NOC)

The results of these metrics during an OO development effort are inputs to the technical risk management and assessment program. Trends which do not meet industry best practice or an external (customer) or internal goal are fair game for a risk write-up.

It is evident that software risk management is not much different from hardware risk management. The focus must be on processes up front and early during the engineering/development cycle. TPMs are excellent early indicators of potential risk and should be used as inputs to the risk identification process. Although conventional

software development methods are being replaced by OO methods, there is still the need for performance measures which are linked to the technical risk management and assessment program.

F. VALUE OF RISK MANAGEMENT

There is significant value and pay-off to implementing an effective risk management and assessment program supplemented with independent risk assessments. It ensures a complete, comprehensive, and integrated approach. Internal risk management programs usually emphasize product and technology risks. They do not do an adequate job of identifying process and programmatic risk. This is where independent risk assessments help fill the gap and ensure a complete (and total) program risk assessment. The following statements summarize the value of risk management (and assessment):

- Provides a systematic decision-making process that efficiently identifies risks, assess risk levels, and effectively reduces or mitigates risks to achieve program goals.
- Provides a proactive risk management & assessment approach to identify potential problems or risks early on where they are much more cost effective to manage and mitigate.
- Implements a demonstrated and proven methodology used on many DoD and commercial acquisition programs.
- Implements best industry practices, lessons learned, and engineering fundamentals, critical disciplines, and process rigor.
- Applies a complete tool set of qualitative and quantitative risk assessment methods to provide the desired level of insight for decision makers.
- Provides timely insight to potential risks that could adversely affect key/critical program milestones if left unmitigated.
- Assesses the risk of new technologies, unproven processes, and COTS/NDI selection and use.

G. RISK METHODS TAUGHT AT DAU

Formerly Defense Systems Management College (DSMC), Ft. Belvoir, VA is home to the Defense Acquisition University (DAU). DAU provides acquisition training and certification to both military and civilian members of the acquisition workforce. DAU also publishes many DoD acquisition guides and maintains the *Defense Acquisition Deskbook*, which is a complete acquisition knowledge information system and reference library available on the web and compact disc.

DAU has published for five years now a *Risk Management Guide For DoD Acquisition*. The latest (5^{th}) edition was released in June of 2002. The risk methods contained in this Guide are taught at DAU. They focus on an Integrated Product and Process approach to risk management and assessment similar to the guidance in NAVSO P-3686, which is also referenced in this Guide. The Process approach is based on the Willoughby Templates and a best practices strategy. The Product approach is based on the WBS and the resultant product decomposition where the risk events that might have a negative impact on the system, subsystem, or components as defined by the WBS are evaluated (DAU, 2002, p. 57). Both the Process and Product based approaches are qualitative in nature and require a subjective classification method to arrive at a risk level. DAU recommends the 5 X 5 Matrix Method. The overall risk level is determined by the intersection of the probability of occurrence and consequence of occurrence values.

With this Guide DAU also teaches the Cost and Schedule Risk Analysis techniques which utilize a Monte Carlo simulation on the WBS and project schedule. These are considered quantitative methods and are not addressed NAVSO P-3686. The other quantitative method, PRA, described in the Total Program Risk Model is not discussed in either the Guide or NAVSO P-3686.

As with NAVSO P-3686, the Guide advocates a risk management organization with the risk manager reporting directly to the program manager. It also recommends the use of independent risk assessors reporting to the program manager.

Software risk management is briefly mentioned in the Guide, and it takes a best practices approach. The guide makes no distinction between the management of software and hardware risk. The process is the same. The Guide provides three best practices methods for software risk management taken from an Air Force guide. (DAU, 2002, pp. 88-92)

Overall, DAU and the latest Risk Management Guide provide a good comprehensive overview of risk management and assessment techniques. They provide good coverage of qualitative and quantitative techniques including software. It is recommended that in future guidance and updates to the Guide that PRA methods be discussed. In addition, classes devoted and dedicated to risk management and assessment techniques should be offered through the DAU curriculum. Often risk management is offered as simply a short module in another curriculum. It is recommended that separate risk management and assessment classes be established.

H. TECHNICAL RISK MANAGEMENT WITHIN THE SYSCOMS

1. NAVAIR

NAVAIR has institutionalized the requirement for technical risk management by making it a key component of their systems engineering technical review process. NAVAIR has a technical process review manual that requires that technical risk assessments be conducted prior to technical design reviews and major milestones throughout the life cycle (CAPT M. Patterson, personal communication, August 9, 2002). This amounts to approximately 12 required technical risk assessments throughout the systems engineering process/life cycle for a typical NAVAIR acquisition program.

NAVAIR's recent focus is on standardization of risk management methods. Every PEO seems to do risk management and assessment differently. Many use the 5 X 5 Matrix Method tailored specifically for each program. Most programs have risk review boards that meet monthly to discuss risk identification and mitigation status. High-level risks are generally managed at the program level, and Low risks are managed or watched by the IPTs. Some PEOs and program offices (PMAs) promote a risk

awareness culture with full, open, and honest communication of risk status. Others do not like to disclose High risk (red) areas. In an effort to standardize across the PEOs, NAVAIR is currently working on a draft risk management instruction and handbook. This instruction will require that all programs have a risk management program and provide standard classification and reporting formats. The standard classification format will be the 5 X 5 probability of occurrence versus consequence matrix. NAVSO P-3686 is being used as a guide to develop this standard risk management process.

NAVAIR already has an instruction for system and safety risk management. System and safety risks are automatically escalated to the program manager for management. Probabilistic methods (e.g., fault tree, event tree, etc.) are used as inputs to the technical risk management and assessment program and are rolled up into the 5 X 5 Matrix for classification.

NAVAIR will soon supplement its systems engineering qualification process curriculum to include an 8-hour module on technical risk management. Currently, only about an hour of risk training is offered. NAVAIR realizes they need to do more training on technical risk management.

2. NAVSEA

NAVSEA lacks an overarching policy statement or instruction for risk management. As a result, some of the PEOs have issued internal instructions and guidance on risk management methods. For instance, Program Executive Office for Theater Surface Combatants (PEO TSC) has published an instruction on risk management (PEOTSCINST 3058.1). This instruction provides policy and guidance for a common risk management process for all PEO TSC programs (PEOTSC, 2000, p. 1). It focuses on qualitative risk assessment techniques only and requires the use of the 5 X 5 Matrix Method to classify risk. The instruction mandates the use of TRIMS and *Risk Radar* as the common toolset and risk database. TRIMS provides an identification, mitigation, tracking, and reporting tool for process-based risk. *Risk Radar* provides a Microsoft Access based risk database for tracking product and software risks. PEO TSC

is commended for attempting to standardize risk management approaches for all its programs resulting from the lack of policy from NAVSEA. However, they have not yet considered the value of quantitative methods. This is no different than what most NAVSEA programs have done concerning quantitative risk management and assessment methods.

An interview with two high-level risk management professionals within the NAVSEA organization who wish to remain anonymous has substantiated what this author has suspected for a long time. NAVSEA acquisition programs primarily focus on the identification and mitigation of Product risks. In other words, they do not focus on the process-based risk early in the life-cycle which has proven to lead to Product risk. The interviewees indicated that in general quantitative methods, such as Cost and Schedule Risk Analysis and PRA are not being used within the NAVSEA community.

Why the primary focus on Product risks? The answer lies in who is identifying a majority of risks on a program. Program IPTs are tasked in many cases with identifying risk. These IPTs are usually chaired by the contractor and are inherently product based. This means the IPT is formed around a particular product or piece of hardware. Therefore, it is only natural for IPT members to focus on hardware (product) specific risk. However, as we have seen from NAVSO P-3686, the most effective risk management and assessment program is an Integrated Product and Process based approach. Process risks should be identified early during design and development to ensure the proper engineering disciplines are being applied. Because the contractor(s) most always focus on Product risk, Navy program managers sometimes hire independent risk assessment teams from the field activities to assess the Process risk on the program. NAVSO P-3686 (1998, p. 8) recommends independent risk assessors be part of the risk management organization reporting directly to the Risk Management Coordinator. Unfortunately, the independent teams are often called in much too late in the life cycle, generally during EMD, to support the MS III production decision.

The use of independent risk assessors is rare within NAVSEA. In contrast, some SPAWAR program managers use independent risk assessment teams as early as the source selection process to ensure the prospective contractors have the proper

engineering disciplines in place to avoid risk. These program managers retain the services of their independent risk assessment teams throughout the life cycle to conduct risk assessment snapshots on the selected contractor/activity. Independent risk assessment teams conduct process-based assessments and the contractor(s) conducts product-based assessments. Both teams share the same risk database and are fully engaged in the status of all identified risks. Representatives from both teams participate in a monthly risk review board to discuss risk identification and mitigation status.

The use of the 5 X 5 Matrix Method and the overall risk level cube tailored by each program office are the predominate methods used on NAVSEA programs. These methods provide for a quick and easy technique for assigning risk levels, albeit subjective in nature. There are also variants of the 5 X 5 method being used by others. Raytheon Missile Systems in Tucson uses a 10 X 10 matrix, which is shown in Appendix B.

The lack of quantitative methods within NAVSEA has already been discussed, but one interviewee believes PRA methods should not be done by independent risk teams, but only by contractor design and systems experts. The interviewee is a Risk Manager for a NAVSEA ACAT I program. Independent risk assessment teams should ideally focus on qualitative, process based methods because they are most often missing in a contractor's risk management program. Contractors should be doing PRA as part of the design and development process because it is an extension of the FMEA process. Conducting "what if" analysis to determine the probability of failure and associated consequence in quantitative form is inherently part of the design and systems engineering process.

What is the feeling of our risk experts on the risk culture within NAVSEA? One interviewee felt that many programs claim to do continuous risk assessment, however they really only do periodic assessments just prior to a major milestone to achieve a check in the box. In other cases, they only care about risk when it comes time to submit a periodic acquisition program status report to a milestone decision authority. It seems that many NAVSEA risk management programs actually track problems not risks. They are practicing problem management not risk management. This means the risk has already occurred (probability is 100%), so it is a problem, which needs corrective action. It

doesn't get management attention until the risk has occurred, and it is now a problem impacting the program that needs to be dealt with. Everyone "talks-the-talk," that is, they pay lip service to the risk management policy from DoD and SECNAV, but when it comes right down to it they don't "walk-the-talk" or execute the intent of the policy and associated guidance.

A sure sign of the level of attention given to risk management within an acquisition program is the status of the risk manager. NAVSO P-3686 (1998, p. 7) states,

> The key to establishing an effective risk organization is to formally assign and empower an individual whose primary role is managing risk. This individual, referred to as the Risk Management Coordinator, should be a higher-level program office person, such as the Deputy Program Manager (DPM), and should be accountable directly to the PM for all aspects of the risk program. The Risk Management Coordinator must have a level of authority which provides direct, unencumbered access to the PM and can cross organizational lines.

Within NAVSEA acquisition programs the status of the risk manager is questionable and inconsistent. There is rarely a risk manager with power. One risk manager interviewed by this author indicated that he rarely gets any feedback at all from the program manager on his risk reports.

For the most part, there is not a risk friendly culture within NAVSEA. Programs want to know their risks, but they don't desire visibility of their risks outside of their program. Contractors also don't want to identify high risks for fear of program schedule or funding delays. On the contrary, contractors should be encouraged and incentivized to identify risks, but this has not occurred within NAVSEA. A "shoot the messenger" culture is still present. Until the high-level decision makers make a point to instill a risk friendly environment with their actions and treatment of those who report program risk, it will be difficult to change the risk culture.

Both interviewees thought that more risk management and assessment training was needed in the NAVSEA community. Training should consist of both qualitative and quantitative methods. They seemed to be in agreement that for quantitative methods, Cost and Schedule Risk Analysis should be the primary focus prior to PRA methods.

Training should be conducted jointly with contractor and government personnel in the same class. This will ensure the development of a common language and understanding of the risk methodologies and application strategies for the acquisition program. Both interviewees were advocates of a single risk management process and a joint government/contractor risk database for a particular acquisition program. One interviewee said there are over half a dozen risk databases on his program and none of them can talk to each other. A single, unified risk database should be the norm.

When asked about sources of risk management training, both interviewees recommended DAU and NSWC Corona Division. Both activities have been training acquisition professionals for a number of years.

Finally, the interviewees were asked where they thought NAVSEA was going with risk management. One thought NAVSEA was headed down the path of problem management instead of risk management. He believes NAVSEA needs to release a structured policy statement with guidance on risk management to the community. He recommends a similar approach to what NAVAIR has done, making risk management and assessment inherently part of the systems engineering technical review process. The other interviewee believes NAVSEA needs to continue moving forward and empower everyone in the community to identify and report risk. NAVSEA needs to instill a risk friendly culture so individuals will identify and report risk without risk of reprisal.

3. SPAWAR

SPAWAR lacks an overarching policy statement or instruction for risk management. SPAWAR is currently working on adopting a standard process for risk management across the PMWs (program offices), which will be released as a policy or guidance document. The standard process will be modeled after the risk management approach PMW 189, *Naval Electronic Combat Surveillance*, has implemented across its 5 programs. PMW 189 is considered a leader for risk management application and is a premier organization within SPAWAR, not only for risk management, but also for software best practices, earned value management, and high performance organization.

PMW 189 is part of the PD 18 *Intelligence, Surveillance, and Reconnaissance* Directorate which has two other PMWs that are risk management advocates and practitioners -- PMW 182, *Mobile Surveillance Systems (SURTASS)*, and PMW 183, *Advanced Deployable Systems (ADS)*. The ADS Program participated in ASN(RD&A)ABM's Risk Management Survey of 1997 ((ASN(RD&A)ABM, 1997, p. 2). Both the ADS Program (PMW 183) and the Deputy Program Manager for PMW 189 (when he worked for PMW 163) contributed to the guidance in NAVSO P-3686 (NAVSO P-3686, 1998, p. v). SPAWAR boasts clear leaders in the risk management arena. Let's examine what PMW 189 has done to make themselves a model for all other program offices.

The Deputy Program Manager for PMW 189 was interviewed to discuss his very successful approach to risk management (F. Doherty, personal communication, August 26, 2002). The two most critical elements required to establish and sustain a successful risk management program is leadership and training. Good leadership is required to continually drive the risk efforts and provide constant reinforcement to prevent the risk program from atrophying. It all starts at the top with the PM. The first key to success is the PM must support risk management. PMW 189 assigns dedicated Risk Officers within each of its programs, support centers, and contractors. It is their job to provide this leadership. Risk Officers must have a questioning mind to drive and sustain risk management and assessment efforts.

Training is another key aspect of a successful risk management approach. Both the Navy and contractor Risk Officers take a week long risk management class where they attend in joint session in order to arrive at a common understanding of the risk management language and process. A 3-day risk management course is given to the rest of the program community in joint fashion as well. Risk management training is not a one-time occurrence, but should continue periodically to reinforce risk management functions and to refine, improve, and evolve risk methods.

PMW 189 has also experimented with contract incentives for using risk management. In one contract they put in the contractor's award fee a clause stating if the contractor performed effective risk management, then at least 25% of the award fee had

to be shared with all the employees in the company. This was great way of incentivizing the entire company workforce to identify and mitigate risks. There was no hiding of risks here! The success of this incentive structure serves as a model for other programs to use.

PMW 189 considers risk management a key program manager responsibility. As a result, the PMs and Risk Officers have risk management performance criteria in their performance appraisals. The contractors also rate the performance of their PMs on risk management and assessment effectiveness. Openly declaring a risk is good, and hiding a risk is bad. A no surprises approach is rewarded. Those PMs and Risk Officers that don't take risk management and assessment seriously are penalized.

As NAVAIR has done, PMW 189 has made risk reporting a key focus of all program and baseline reviews. They use the stoplight, color-coded approach to present the risks with supporting details. Weekly risk updates are provided to the PMs with a monthly in-depth review. *Risk Radar* is used to catalog the risks. Thus, PMW 189 has fully institutionalized the risk management process within the acquisition life-cycle, the systems engineering process, and the program management discipline

Qualitative risk assessment methods are used primarily by PMW 189. They use informal methods based on expert opinion and some check sheets. They don't use a templates or best practices approach (except for software risk). They believe people will find the best practices through innovation and discipline. They assess all types of risk including software, hardware, and process related risk. Their software risk assessment approach is based on software best practices. They have very clear definitions for risk, and they use the 5 X 5 Matrix Method to classify risk. They are advocates of keeping the risk assessment and classification process simple or people won't use it. This is the reason why they like the 5 X 5 Matrix Method. They do very little quantitative risk assessment. Cost and Schedule Risk Analysis using Monte Carlo simulations are not used. One PRA method using fault tree analysis is used to some extent to drill down to a level where the risk can be assessed more appropriately. Then, like NAVAIR, they use the output from PRA as an input to a qualitative assessment. This is not a pure application of PRA as NASA uses it, but a good start.

PMW 189 has effectively implemented risk management and assessment. A constant focus on risk assessment driven by strong leadership and a good understanding of risk by the community resulting from frequent training has been the key. This diligence saved one program helping it pass OPEVAL. The success of PMW 189 has not gone unnoticed. Other PMWs have asked for assistance in setting up risk management and assessment programs. Some contractors have come to PMW 189 asking for independent risk assessments because of their knowledge in this area. Finally, SPAWAR has recognized PMW 189 as a model for the entire organization and is in the process of writing a risk management and assessment policy and guidance document using their methods.

The jury is still out concerning where SPAWAR is heading with risk management. There are some pockets of success, but it has not been institutionalized across the SYSCOM.

I. CHARACTERISITICS OF RISK MATURE ORGANIZATIONS

How does an organization know when it has reached a level of risk maturity comparable to today's world-class risk management leaders? Hullet (2001, p. 7) provides a list of key characteristics, which are worthy of repeating here:

- Organizational culture is "risk friendly."
- Risk management gains priority to rank along with cost, time, and scope management.
- Decisions are made and resources are allocated based on the results of risk analysis.
- The highest quality data are used for risk analysis and resources are committed to the efforts.
- Risk management is viewed as a career path in the organization even though that may make it hard to "control."
- Mature risk management organizations look to the best in class to benchmark their risk management processes.
- They use modern tools and are not disdainful of sophisticated and proven approaches.

- They measure their effectiveness with metrics.
- Project decisions are made on a "risk-adjusted" basis.
- Continuous improvement is achieved through regular repetition.
- They participate in professional interchanges through conferences and journals sharing what they have learned.

Using these key characteristics as benchmarks, it is evident based on the results of this Survey and interviews with key risk professionals within the SYSCOMs that the Navy has not yet reached a high-level of risk maturity. In contrast, NASA seems to have reached a level of risk maturity. Why? Risk management is viewed as an important part of project management and the status and rank of risk management responsibility is equal to that of program management. NASA utilizes modern risk management and assessment tools, such as PRA, and is continuing to develop and hone probabilistic methods. There appears to be a "risk friendly" culture within NASA; however, within the Navy there is still a risk-hiding culture for fear of surfacing bad news.

III. TECHNICAL RISK MANAGEMENT SURVEY

A. WHY SURVEY?

Acquisition reform brought with it a major change in how the acquisition community views risk. ASN(RD&A)ABM's survey of Navy program managers in 1997 revealed an increased awareness of technical risk; however, risk management and assessment methods were not common, nor completely institutionalized throughout Navy programs. The results of this survey led to the publication NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*, a comprehensive technical risk management guidance manual in 1998 by ASN(RD&A)ABM. NAVSO P-3686 was written for program managers and other acquisition professionals to provide a common, best practice approach to technical risk management and to address the deficiencies noted in the 1997 survey.

Now that NAVSO P-3686 has been widely publicized and available to the acquisition community for nearly 4 years via many sources including the *Defense Acquisition Deskbook*, ASN(RD&A)ABM's Web Site, Defense Contract Management Agency's Web Site, and DAU. A primary objective of this thesis is to determine if NAVSO P-3686 is being used by Navy programs to establish technical risk management functions. As part of this thesis research, a Survey was conducted of program managers and other acquisition professionals to determine their attitudes towards technical risk, the methods and techniques being used, and guidance documents used to establish their technical risk management and assessment programs. The Survey specifically examined if NAVSO P-3686 was being used.

B. THE SURVEY

The Technical Risk Management Survey consisted of 30 questions, with roughly one half of the questions using a 5-point Likert scale. The other half were Yes/No and open-ended fill in the blank type of questions. The Likert technique is based on a set of attitude statements. Respondents were asked to express agreement or disagreement with

a statement concerning some aspect of risk management and assessment. Each degree of agreement is assigned a numerical value from one to five. ("The Likert scale," n.d., ¶ 1) A copy of the Technical Risk Management Survey is provided in Appendix E.

In order to maximize the probability of the Survey being completed and returned by respondents, an efficient and user friendly surveying method was chosen to minimize the impact on already busy acquisition professionals. A web-based survey hosting tool, called Zoomerang (www.zoomerang.com), was selected to create and distribute the survey. Zoomerang also provided the tracking of respondents and collection and reporting of survey results. The Survey was recreated within Zoomerang using radio buttons and drop down menus to select attitude statements and Yes or No question responses. Scrollable text boxes were used for the open-ended question responses. The end result was a simple point and click approach to filling out the Survey using any Web Browser. The estimated time to fill out the Survey was 10 to 15 minutes. The Survey was prefaced with an introductory paragraph describing the purpose of the Survey, followed by the 30 questions. After completing the Survey and clicking the "Send" button, a thank-you page appeared with the author's name and phone number. Respondents who would like to see a copy of the Survey results were encouraged to call the author and request a copy of the thesis.

C. SURVEY EXPOSURE

In order to make suppositions about technical risk management attitudes and application within the Navy, a good cross section or sample of program managers and acquisition professionals was necessary from each of the three SYSCOMs (NAVSEA, NAVAIR, and SPAWAR). In addition, since risk management and assessment functions are sometimes delegated to support contractors or led by prime contractors, a sample of contractor personnel was also surveyed.

Zoomerang's primary method of launching a survey is via E-mail addresses. The Technical Risk Management Survey was E-mailed to 69 invitees across the three SYSCOMs, including support contractors and prime contractors. Zoomerang

automatically generates an E-mail with introductory text provided by the author. After the introductory text, Zoomerang provides a hyperlink to the Survey, so the invitee simply has to click on the hyperlink within the E-mail to get to the Survey. Zoomerang keeps track of who has responded by E-mail address. Automated weekly E-mail reminders are sent out to those on the initial mailing list who have not yet responded.

Zoomerang allows the posting of a survey link on a Home Page or Web Site. This method was also used for the Technical Risk Management Survey to gain maximum exposure. BMPCOE graciously agreed to host a hyperlink to the Survey on their Web Site under *News & Events*. BMPCOE is a primary source of technical best practices for government, industry, and academia. Their Web Site provides on-line access to over 2,500 proven best practices including knowledge information and risk management/assessment tools which are also available for free download. Thanks to BMPCOE, the Technical Risk Management Survey was subjected to a wide exposure. Appendix F shows a link to the Survey on the BMPCOE Web Site.

The Survey was officially launched on July 15, 2002 and remained active for 35 days until it closed on August 18, 2002. A majority of responses were received within the first 10 days, although a few respondents replied during the last two days of the active window. The weekly-automated E-mail reminders were very useful in capturing the stragglers.

D. SURVEY RESULTS

A total of 69 invitations were sent to program managers and other acquisition professionals across the three SYSCOMs. Over the course of the 35-day active window, there were 38 respondents for a response rate of 55%. This is much better than the average response rate of 36.83% to E-mail surveys over a 15-year period (1986-2000) as reported by Sheehan (2001, Results). The significant highlights and trends of the Survey will be summarized in the following paragraphs. A complete copy of the survey results is contained in Appendix G.

1. Experience Levels of Respondents

The Survey asked a few questions concerning the experience levels of the respondents. The results were positive. The Survey respondents were very experienced in systems acquisition and support. Almost all of them were certified to a DAWIA Career Field with the most frequent being Level III Program Management (PM), followed by Level III Systems Planning, Research, Development, and Engineering (SPRDE), and finally a few Level II and III Production, Quality and Manufacturing (PQM) categories. The respondents averaged 16 years of acquisition experience and 10 years of risk management experience. Of the 38 total respondents, 10 indicated a title or position of program manager and 5 could be considered risk managers. The remaining 23 were acquisition professionals working within program offices, for prime contractors, or supporting field activities and contractors. Of the 10 respondents identified as program managers, 3 were affiliated with NAVSEA, 1 with NAVAIR, 4 with SPAWAR, 1 with a prime contractor, and 1 unknown (could not be traced). Of the 5 identified as risk managers, 2 were affiliated with NAVSEA, 2 with NAVAIR, and 1 with SPAWAR.

2. Respondent Affiliation

A good cross section of acquisition professionals was surveyed across the Navy SYSCOMs and supporting organizations. Of the 38 respondents, 42% were affiliated with NAVSEA, 24% with SPAWAR, 21% with NAVAIR, and 26% were classified as "Other." The "Other" category included prime contractors, subcontractors, and program office support contractors. The NAVSEA response was approximately twice that of the other SYSCOMs because most of the field activity respondents were affiliated with NAVSEA.

3. Technical Risk Management Attitudes

A number of Survey questions dealt with respondent's attitudes towards technical risk management and associated methods. Survey questions # 1-6, # 10-11, # 16, and # 28 are grouped under this category.

When asked about the importance of technical risk management to the success of a program, 100% of the respondents rated it Important or higher. 55% rated it Extremely Important and 37% said it was Very Important. These results substantiate one of the conclusions of ASN(RD&A)ABM's 1997 Risk Management Survey which said that there was an increasing awareness within the Navy community concerning technical risk. Without a doubt, this is certainly true today and supported by the Survey results.

Acquisition reform initiated a change from a risk avoidance culture to a risk management culture. Risk management became a key component of program management and a key tool for the program manager's tool kit. When asked if the respondents believed technical risk management was a key component of program management, 71% Strongly Agreed with this statement. The remaining 29% Agreed with this statement, which left no respondents selecting the Neutral or Disagree attitudes. These results indicate that program managers certainly understand the value of technical risk management, and it should be part of their program planning and execution.

The next series of questions asked the respondents how they felt about the effectiveness of the qualitative and quantitative technical risk management methods describe previously in this thesis. Qualitative methods based on a Willoughby Templates and best practices approach were rated Very Useful by 50% of the respondents. Only 18% rated these methods as Extremely Useful, 21% said they were only Useful, and 0% said they were Not Useful. Quantitative methods, such as PRA and Monte Carlo simulations, were rated somewhat lower with 26% rating them Very Useful, 13% Extremely Useful, and 5% Not Useful. However, the middle categories of Useful and Somewhat Useful rated higher for the quantitative methods. These results substantiate the contention that qualitative methods are the predominate technical risk assessment

methods within the Navy today. It is encouraging to note that respondents must be aware of quantitative methods because no one selected the Don't Know category.

In an effort to determine if respondents believed there is a correlation between systems engineering and technical risk management one Survey question asked if a systems engineering approach better manages or minimizes technical risk. 61% of the respondents said absolutely and Strongly Agreed. 34% Agreed and surprisingly 5% responded with Neutral. Fortunately no one Disagreed with this statement. With many of the respondents certified to the DAWIA Level III SPRDE and PM categories, it is surprising that there was not a more overwhelming majority for Strongly Agree. This thesis has made the contention that there really is no difference between the critical engineering processes outline in a risk templates approach and the systems engineering disciplines. In fact, technical risk assessment should be used to measure how effectively the systems engineering disciplines have been implemented. The variance between current practice and best practice determines the risk level.

This discussion on best practices and critical engineering processes is a good lead in to another related Survey question, which asked if systematic and proactive identification and correction of faulty processes would reduce the occurrence of downstream acquisition problems. 50% of the respondents Agreed that a proactive correction of faulty processes would indeed prevent future problems from occurring. 47% Strongly Agreed with this statement. These results indicate that acquisition professionals do understand the importance of early identification and mitigation of process based risk. A key theme in this thesis is unmitigated Process risk leads to Product risk. The question remains why do many acquisition programs not implement proactive and aggressive risk management programs if they understand the benefits of early identification and mitigation? The answer may lie in reduced budgets, the difficulty in quantifying the downstream savings of early investment in risk management and assessment, and a lack of incentives to apply risk management and assessment techniques.

For years the biggest argument from program managers is "show me my savings from my up front investment in risk management before I commit to an aggressive risk

program." It is not easy to quantify the savings from a risk management program. Intuitively we know if risks are identified and mitigated early, future problems are avoided. It is difficult to estimate the cost of a future problem, plus it takes time that many do not have to perform the estimates, if it can be done at all. The Survey asked the respondents to estimate the savings from their risk management programs to see what kind of responses would be obtained. As suspected, the respondents had significant difficulty with this question. Of the 24 who responded, 20 could not provide an estimate. Here is what some had to say:

- "Savings a Risk Management Program provides cannot be measured."
- "Savings are hard to pin down – the success of the program is the only real metric that gets high visibility with me."
- "That is too hard. It's cost avoidance and grief avoidance."

The four that did respond had the following to say:

- "This is hard. I'd say $2 to $3M/year for technical risks. It could be much, much higher for the tactical risks (say an order of magnitude)."
- "Impossible to calculate savings, but I would guess on the order of 10-25% of total acquisition cost."
- "100K-$500K (ROM)."
- "$400-500K."

A good topic for further study would be to develop a model for program managers to use to quantify the cost savings from their risk management program.

Respondents were asked if they perceived risk management as a source of workload instead of part of the acquisition solution. 45% Disagreed that risk management was a source of workload. 11% Strongly Disagreed. However, surprisingly 26% of the respondents Agreed that risk management was a source of workload with 5% Strongly Agreeing. 13% were on the fence with Neutral. Thus, nearly one-third of all

respondents believe risk management is simply a workload task. If you throw in the non-committals you are approaching 45%. This is a surprising result considering 100% of the respondents believed technical risk management was Important or better (Very or Extremely Important) to the success of an acquisition program. This can be interpreted as they think technical risk management is important, but they don't like doing it, perhaps because it is not easy.

Finally, attitudes towards specific features of a technical risk management program were surveyed. One of the NAVSEA risk professionals interviewed as part of this research indicated there were over half a dozen individual risk management databases on his program. None of the databases could talk to one another and in order to roll up total risk on the program, reports from each database had to be prepared and consolidated into one report. This is a good example of why a single joint program office/contractor risk management program and database is highly recommended. It is important that the entire program community speak the same language and share the risk management process. As a result, one Survey question asked how important is a single risk management program and database for an acquisition program. 32% responded Extremely Important, 39% said Very Important, and 24% rated them Important. Only 3% said they were Not Important.

The other feature of a risk management program surveyed was whether or not risk mitigation plans should be loaded into the WBS/Project Schedule. 32% Strongly Agreed that they should be fed back into WBS/Project Schedule, 34% Agreed, 21% were Neutral, 11% Disagreed, and 3% Strongly Disagreed. What is surprising is that 14% of the respondents Disagreed that risk mitigation plans should be factored into the project schedule. This is often the reason why risk management programs are ineffective. If risk mitigation plans and resources are not properly planned for by incorporating them into the project schedule, then mitigation doesn't get budgeted or implemented. This is a significant oversight by nearly 15% of the programs surveyed and may be the root cause of their dissatisfaction with their risk management programs (see paragraph 10).

4. Acquisition Reform Impact on Technical Risk Management

This thesis has discussed in depth the impact acquisition reform has had on technical risk management attitudes, policies, and methods. Survey questions # 7-9 are grouped under this category.

We asked a simple question. Did acquisition reform increase the need for technical risk management? 55% Strongly Agreed with this statement, 24% Agreed, and 8% were Neutral. Surprisingly, 8% Disagreed and 5% Strongly Disagreed with this statement.

Acquisition reform brought with it a change in the risk culture which resulted in an evolution of risk methods. The Survey asked respondents if they thought technical risk management methods & techniques have changed drastically in the last 15 years. 32% Agreed with this statement, but 26% said they Did Not Know. 16% Strongly Agreed, 18% were Neutral, and 8% Disagreed.

The Survey asked each respondent if they believed there was a risk awareness culture within their program office where program risks are identified and openly discussed. It was encouraging to see that 32% Strongly Agreed, and 30% Agreed. However, 22% were Neutral, 14% Disagreed, and 3% Strongly Disagreed. Thus, 17% said there is not a "risk friendly" culture within their program office. Adding in the neutrals, that's nearly 40%! These results substantiate what the SYSCOM interviewees described in their interviews that there are program offices where risks are not openly discussed.

5. Software Risk Management Methods

This thesis has established the importance of a disciplined approach to software development. Because software engineering needs a disciplined process, a process-based technical risk assessment strategy is necessary to measure how well software engineering disciplines have been implemented. Ineffective process-based risk assessment on the

software engineering process will lead to software Product risk. The Survey asked two questions associated with software risk management attitudes. Survey questions # 12 and # 13 are grouped under this category.

First of all, respondents were asked if their risk program included software. 69% said Yes and 31% said No. Thus, nearly one third of program offices are not measuring the performance of software development. Nearly all programs today use software products, so this oversight is critical. The respondents were then asked what software risk management methods they used. The responses were varied from software metrics to checklists. There were a number of TPM responses which included standard software industry performance measures, such as lines of code, CPU usage, memory usage, I/O channel usage, function points, etc. The types of checklists used also varied from the Willoughby Templates, TRIMS, and best practices to the Software Program Manager's Network (SPMN) 16 Critical Software Practices and internally created program checklists. One respondent created checklists tied to the systems engineering technical reviews (e.g., SRR, SFR, PDR, CDR, PRR, etc.). Another used DoD's PM Guide to Software Acquisition Best Practices. One respondent utilized an independent software engineering team and another conducted a software fault tree analysis. Surprisingly, only one respondent mentioned the use SEI's SW-CMM. Many also mentioned the use of *Risk Radar*, which is a risk management database tool that helps program managers to identify, prioritize, and report program risks in a user friendly format (SPMN, n.d., ¶1). The Survey results show that there are pockets of software risk management occurring, but most is based on qualitative approaches with few quantitative metrics. Nearly one third of those surveyed don't even apply software risk management methods.

6. Technical Risk Management Guidance

One of the objectives of this Survey was to determine what guidance documents for technical risk management are being used within the Navy acquisition community. Of particular interest was how often programs were using the Navy's premier guidance document on technical risk, NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*. Survey questions # 14, # 15, # 25-27 are grouped under this category.

One question addressed NAVSO P-3686 directly and asked the respondents if they were using this document as guidance for their risk management programs. The respondents were split on this issue with 36% saying Yes and 36% saying No. 28% said they Did Not Know. When asked how many have used DoD 4245.7-M (Willoughby Templates), NAVSO P-6071 *Best Practices*, or *Methods & Metrics for Product Success* as guidance for risk management, 44% said Yes and 28% said No. Once again, 28% said they Did Not Know. The results indicate that more respondents are familiar with the Willoughby Templates than NAVSO P-3686. As we have discussed previously, NAVSO P-3686 is a culmination of all previous Navy technical risk management guidance including the Willoughby Templates. The difference may simply be attributed to the fact that the Templates have been around for 17 years and NAVSO P-3686 only four years.

In another survey question respondents were asked to list the technical risk management guidance documents they are familiar with and using on their programs. The following documents provide a sample of the responses:

- NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*
- BMP Guides
- DoD 4245.7M (Willoughby Templates)
- TRIMS
- NAVSO P-6071, *Best Practices*
- *Methods & Metrics for Product Success*
- DoD 5000.1, DoD 5000.2, DoD 5000.2R
- SECNAVINST 5000.2
- DAU *Risk Management Guide for DoD Acquisition*
- FAR
- Defense Acquisition Deskbook
- NAVAIR instructions, handbook materials, and checklists

In a related question, respondents were asked what risk management documents are being used by their contractors. Many said they were not sure or simply said various documents. Some said they used their own internal policy. Others said they use the same documents as the Navy program office. The surprising trend is that approximately 70% of the respondents had no idea what risk management policy and guidance documents their contractors were using. The other 30% used the same guidance documents as the Navy program office.

7. Risk Management Policy

Two of the three SYSCOMs, NAVSEA and SPAWAR, have apparently not issued any type of risk management policy statement or guidance document. As a result, program managers have had to rely on higher-level policy statements from DoD and SECNAV. Survey questions # 25-27 are grouped under this category.

The Survey asked respondents if they felt DoD, SECNAV, and NAVSEA policy adequately addresses risk management requirements. 43% Agreed that it was adequate, but 40% were Neutral on this statement, and 17% Disagreed. No respondents Strongly Agreed or Strongly Disagreed. These results indicate that there is room for improvement in high-level risk management policy.

8. Risk Management Training

A number of interviewees indicated the importance of training to the technical risk management effort. Survey questions # 21-23 are grouped under this category.

The Survey asked respondents if they have received risk management training. 82% of respondents said Yes with 18% saying No. This is an encouraging result, but nearly one in five (20%) have had no training at all. However, just because 82% said they have had some kind of risk management training, this doesn't mean they don't need additional training. Recall, the model organization for risk management within SPAWAR (PMW 189) believes risk training is an on-going process.

The Survey asked, where was the risk management training acquired and what methods were taught? DAU was the most frequently cited source of risk management training. However, this training was received as part of one of their program management courses. The second most frequently cited source of risk management training was NSWC Corona who has provided risk training and assessment services to various SPAWAR and NAVSEA program offices, as well as contributed to various ASN(RD&A) technical risk management guidance documents. The SPAWAR respondents cited SPMN as a good source for risk management training. Dr. David Hullet's class on Cost and Schedule Risk Analysis was referenced a few times, as well a Brian Willoughby's class on BMP and TRIMS. All but one of these sources predominantly focuses on qualitative methods. Dr. Hullet's class examines two of the non-technical quantitative methods as illustrated in our Total Program Risk Model discussed previously in this thesis. The most frequent methods taught were those qualitative methods based on the Willoughby Templates and *Best Practices* guidance documents. The TRIMS tool which is based on the Templates and best practices approach was also cited a number of times. The use of 5 X 5 Matrix Method was also referenced frequently. Monte Carlo Cost and Schedule Risk Analysis methods were cited half a dozen times. *Risk Radar* and risk (fault/decision) tree analysis were referenced a couple of times. One response indicated a clear use of PRA methods. A SPAWAR respondent referenced the use of classroom training and risk management symposiums with their contractors and Systems Centers in addition to top management training. The program office for this respondent conducted a risk identification session for all of SPAWAR with the SYSCOM Commander participating. The results indicate a good variety of both qualitative and quantitative technical risk management methods being taught by providers, however it appears that not all methods are being applied in the field.

9. Risk Management Program Elements & Successes

The Survey asked respondents what were some of the key elements of their risk management programs. Survey questions # 18 and # 19 are grouped under this category.

The following is a sample of the responses:

- "Strong government encouragement of culture open to identifying risks; joint government/contractor risk reviews, technical subject matter experts from government and university labs; TRIMS database and lessons learned; process rigor by asking the tailored, detailed TRIMS questions."
- "Systems engineering approach; all players at the same table (processes, contracts, logistics, engineering, test and evaluation, post IOC support, manufacturing, R&M, systems safety, quality, E3, survivability, software, etc."
- "On-going, iterative, and integral to management of the program."
- "Fostering an environment for teams to identify risk."
- "Our Risk Management Program is primarily an action tracking system for maintaining visibility of identified risks."
- "We have a Program Office Risk Guide document that lays out some guidelines for monitoring Risk on a program. We include the contractor and the TDA in our Risk identification and tracking method, called our 'Risk Radar'."
- "Product/Process Production Readiness based look at potential traps by asking the appropriate questions."
- "Periodic safety reviews by WSESRB, risk assessments for flight clearance, and software/hardware weapon fuzing risk reviews."
- "Applying knowledgeable and empowered personnel to address a myriad of issues and challenges within programs."
- "Risk Radar Data Bases, and risks are reviewed at all program reviews. We have a risk policy and risk officers. We have trained all our personnel on risk management."
- "Holding joint Risk ID sessions with the contractor and all Govt. support organizations. One full day of our quarterly program review is dedicated to identifying any new risks and development of mitigation and contingency plans."
- "Risk Reviews."
- "Incorporation of the results from SVRs and other reviews into the risk management system."
- "Proper visibility of the risks at the SEMT level."

- "The Risk Radar Database; fairly rigorous Risk Identification process; weekly review by APM with his team of risk status; bimonthly face-to-face review of risk status with upper management."
- "We help others conduct risk management using our TRIMS/PMWS tools."
- "Communication of all issues to all Risk IPTs."
- "Process & Product based; Joint Contractor/Govt. Risk Database; IPTs are empowered to identify risk; Govt. and industry share the risk."

The Survey respondents were asked to comment on successes they had achieved with their risk management program. The following is a sample of the responses:

- "Clear identification of the highest risk areas and agreement from upper management on mitigation efforts to pursue."
- "Standardized risk reporting/assessment definitions; developed a NAVAIR Systems Engineering guidebook, a Systems Engineering Technical Risk Assessment Process Instruction, and a NAVAIR Risk Management Instruction."
- "We've delivered major subsystems that meet and exceed customer expectations."
- "Good tracking of overall program risk and the ability to understand funding priorities."
- "System has been effective in providing visibility of risks and tracking mitigation efforts."
- "Focus government attention on key contractual events which were key to meeting the program (requirements) and tailoring the SOO and Contract Performance Planning prior to contract award."
- "We've had several successes dealing with identifying Risk associated with new tasking that allowed us to get additional funds into our budget. Also, we identified several tactical Risks that we developed a proposed solution for and then went ahead and tested the solution. In these cases 2 of the tactical risks (mine re-acquisition and depth localization) were successfully mitigated, one (explosive shock) turned out to be unavoidable and is now being worked into our Op. Plan for the system. Most of our successes have been technical. There are too many to list in total here, but for example, we successfully reduced processor overhead (a risk identified early), Electro-static discharge through the towed body, and EMI susceptibility."

- "Smooth transitions in Production Readiness for AEGIS Program Prime/Subcontractors."
- "Successes have varied from program-to-program. Successes are building since formulation and distribution of our risk checklists."
- "We measure success by whether or not a program institutes a formal risk management program with institutionalized processes for risk identification, analysis, reporting, and mitigation. Several have achieved this."
- "We have saved a number of our programs from failure. We are also being led to process improvements. We have a common lexicon across all programs. We have linked performance appraisals to risk."
- "Schedules have been more realistically established that allow for our handling of schedule risks without negative impact to the program or the funding stream."
- "Avoided schedule and cost overruns."
- "Risk management is performed at the IPT level."
- "In one case, we anticipated a loss of financial support for an up-coming experiment, and went out to an alternative sponsor who came through with the funds to allow the experiment to proceed on schedule."
- "We feel that the programs that have used TRIMS and/or the TRIMS methodology (process based Risk Management) have benefited; the more effectively they have used it, the greater have been the benefits."
- "Varies by program observed and is dependant upon the method used. Programs using structured, measurable methods succeed. Programs not using risk assessment fail."
- "COTS Obsolescence risk mitigation, extending the life-cycle of COTS to match that of the program."
- "Successful milestone decisions."

10. Risk Management Program Satisfaction

A key measure of success of a risk management program is how satisfied users are that the program is truly making a positive impact. Survey questions # 17 and # 20 are grouped under this category.

The Survey asked respondents to what degree they were satisfied with their risk management program. The results were surprising. Only 6% were Very Satisfied, 39%

were Satisfied, and 39% were Neutral. 17% were Dissatisfied and none were Highly Dissatisfied. The high number Neutral responses (nearly 40%) indicate that respondents are not getting the results they hoped to get from their risk management program. The Survey asked the respondents what results were you hoping to achieve and where did they fall short with their risk management programs. Some of the responses were informative, yet startling:

- "Still strong risk identification adverse culture at Contractor."
- "Subcontractors continue to be a problem area."
- "We do not predict or forestall risks. We only track them when they occur."
- "There are schedule/cost risks in every WBS element, but we tracked technical risk separately and it wasn't always clear how open technical risk affected overall schedule."
- "We have some program managers totally bought in and others hoping it will go away."
- "I was hoping to have better buy-in from the other Government agencies, but I often find myself doing their risk identification."
- "Cannot control external risks."
- "…we never seem to truly budget for risk mitigation/risk alternatives (i.e., no realistic 'risk reserve'); also, there is always the danger of just going through the reviews without real scrutiny, lulling us into the perception that everything is fine because we are doing risk management, when we can miss the obvious. Maintaining the vigilance is a real challenge."
- "…most of the shortfalls is not communicating the risk from one program to the other when similar process/products are used (e.g., SM-2 BLK III, IV, IVA, SM-3)."
- "Hoping to quantify cost savings due to risk management program. Difficult to overcome the risk hiding culture. No one wants to hear bad news."
- "The results hoped for was actual identification of risk, quantification of risk, and risk mitigation to an acceptable level. Acceptable level does not mean elimination of risk or even reducing all risks to low. It means the risk is manageable."
- "Biggest challenge is to translate the technical risk assessment into terms the PM can understand."

- "Most programs we support that have risk management programs fall short by poorly identifying risks, failure to consider process related risks, and the screening or downplaying risks as they are reported up the management chain."
- "(Hoping to) identify system risks to allow decisions based on total system impact, versus typical situation where most powerful technical discipline 'gets its way'. We still are not able to eliminate skew towards undue weighting of risks to pet technical areas."

These comments and concerns support and substantiate the feedback received from those individuals interviewed within the SYSCOMs discussed in Chapter 2. The comment about failure to budget for risk mitigation activities is a significant issue that can be addressed by proper planning. This thesis has talked about the need to incorporate risk mitigation planning packages into the WBS/Integrated Master Schedule to ensure resources are loaded for risk mitigation activities. Risk identification and development of risk mitigation planning packages must start at the Integrated Baseline Review (IBR) to ensure sufficient resources are loaded.

IV. CONCLUSION

We have seen a tremendous evolution of technical risk management and assessment applications within the Department of the Navy over the course of 17 years. It started with a renewed focus on engineering process discipline and rigor in 1985 with the release of the Willoughby Templates. In 1994, acquisition reform brought with it a risk culture change from risk avoidance to risk awareness and management. Risk management was now considered a key component of program management. With the elimination of military standards and specifications, the Navy no longer had a collection of proven process, practices, and methods to implement to avoid or minimize risk. New acquisition policy and declining defense budgets allowed risk taking and streamlining of acquisition strategies. This increased the need for technical risk management and assessment to gather insight into the effectiveness of contractor processes and practices.

Qualitative (subjective) technical risk assessment methods were used to compare a program or contractor practice with best practice. The amount of variance determined the risk level. Risk levels were classified (assigned) using narrative criteria that often differed significantly among programs. This one-dimensional classification approach soon evolved into a two-dimensional 5 X 5 Matrix Method as the need arose for more proactive assessments of risk due to acquisition reform. The definition of Risk was now comprised of two components: probability of occurrence (likelihood) and consequence (impact) of occurrence. This was an evolution from the earlier one-dimensional definition of risk, which focused only on impact to cost, schedule, and performance.

Quantitative methods evolved to provide a more detailed assessment of risk and the probability of occurrence. The need arose because decision makers desired more quantitative data to base decisions on. There is no opportunity without risk. Quantitative methods include PRA used by the nuclear power industry and NASA, and Cost & Schedule Risk Analysis using Monte Carlo simulations on the project schedule. Quantitative methods have been slow to be adopted by the Navy. Qualitative methods continue to predominate.

Although risk management and assessment is clearly part of a program manager's tool kit today, there is still room for improvement. Technical risk management methods have not been institutionalized throughout the Navy. NAVAIR has recently developed a risk management instruction, but NAVSEA and SPAWAR have not. Because there is no common language, many programs implement risk management differently. ASN (RD&A)ABM's 1998 released of NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*, was an attempt to provide some standard guidance. In four years it has made an impact, albeit slow.

This thesis surveyed a number of program managers, risk managers, and other acquisition professionals within the SYSCOMs to determine their attitudes toward technical risk management and to see what methods and guidance documents they were using. In regards to a program's use of NAVSO P-3686, the Survey found that a little over one-third (36%) of respondents have used or were using this guidance document. The following can also be concluded based on the Survey results:

- Our acquisition workforce is experienced. Respondents averaged 16 years of acquisition experience and 10 years of risk management experience.
- Our acquisition workforce is DAWIA certified. Most of the program manager respondents were or will be Level III certified shortly. Many had a Level III SPRDE secondary certification.
- Despite the respondent's experience and DAWIA education, there is need for more risk management training. Recommend DAU create a separate course for technical risk management and assessment.
- Technical risk management is very important to the success of an acquisition program.
- Technical risk management is a key component of program management.
- Qualitative methods are used predominately within the Navy.
- Training on quantitative methods is needed before significant use will appear within Navy program offices. DAU needs to teach these methods. The Navy should take a look at how NASA has institutionalized PRA methods.
- There is a definite correlation between systems engineering and technical risk management. Technical risk management and assessment methods should be used to measure how well systems engineering and associated disciplines have been implemented on an acquisition program.

- Incentives for technical risk management should be included in contracts. Technical risk management measures of effectiveness or metrics should be included in a contractor's award fee to incentivize the implementation of critical engineering processes and disciplines.
- Program managers have no incentive to do technical risk management. They are often judged and advance in their career by how much they reduce up front costs, not life-cycle costs.
- Unmitigated Process risk leads to Product risk.
- It is difficult to quantify the savings resulting from the implementation of technical risk management and assessment.
- Program managers, risk officers, risk coordinators, and other leaders should have risk management in their performance appraisals. This includes both Navy and contractor representatives.
- Risk management functions are not a source of workload, but a part of the acquisition solution. It may be workloaded early to avoid work later.
- A joint program management office/contractor risk management program and database is recommended.
- Acquisition reform has increased the need for technical risk management.
- Within each SYSCOM there is still not a complete risk awareness culture where program risks are identified and openly discussed.
- The results show that there are pockets of software risk management occurring, but most is based on qualitative approaches with few quantitative metrics. Nearly one third of those surveyed don't even apply software risk management methods.
- The most popular and recognized technical risk management guidance documents in use within the Navy are the documents Mr. Willoughby helped create (DoD 4245.7-M, NAVSO P-6071, *Methods & Metrics for Product Success*). They were cited more often than ASN(RD&A)ABM's latest technical risk management guidance document, NAVSO P-3686, by a margin of 8%.
- 36% of those surveyed have used or are using NAVSO P-3686.
- Approximately 70% of the respondents had no idea what risk management policy and guidance documents their contractors were using. The other 30% used the same guidance documents as the program office.
- There is room for improvement in high-level risk management policy. Nearly 20% of all respondents believed current DoD, SECNAV, and NAVSEA risk management policy was inadequate. Another 40% were Neutral on this issue.

- Nearly 20% of the respondents have not had any risk management training. This begs the question about the climate for training transfer of the 80% that did receive risk management training. Why have they not applied what they learned?
- DAU was cited most frequently as the provider of risk management training, but their risk training is not a dedicated class, but part of other classes.
- Risk management training conducted in joint fashion with Navy and contractor representatives ensures a common understanding and application.
- The Survey results indicate a good variety of both qualitative and quantitative technical risk management methods being taught by providers, however it appears that not all methods are being applied in the field.
- Nearly 20% of respondents were Dissatisfied with their risk management program and nearly 40% were Neutral indicating that respondents are not getting the results they hoped to get from their risk management program.
- Risk mitigation planning packages must be incorporated into the WBS/Integrated Master Schedule to ensure resources are loaded for risk mitigation activities.
- Risk management and assessment methods have not been fully institutionalized within the Navy SYSCOMs. NAVSEA lags SPAWAR and NAVAIR considerably.

Although there is still work to do, the Navy has made strides over the past two decades, moving from a risk avoidance culture to a risk awareness culture. Risk management is a growing discipline and the need is understood by most all acquisition professionals. Risk management is engrained within DoD and DoN policy. The acquisition of defense systems within budget, on schedule (or reduced cycle times), and improved readiness is the Navy's objective. This is achieved through the proactive identification and mitigation of technical risks. The only weaknesses lie in the implementation of risk management and assessment methods and the communication of risk. This author expects aspects to improve in the future, however slowly.

APPENDIX A. RISK IDENTIFICATION FORM

<table>
<tr><td colspan="2">RISK IDENTIFICATION FORM</td><td>XXX-XXXX-###</td></tr>
<tr><td>RISK TITLE:</td><td>Category:
Template:</td><td>FACILITY & PRODUCT/SUBASSEMBLY
Activity:
Product:</td></tr>
<tr><td rowspan="3">REFERENCE</td><td>Date Identified</td><td>DERIVED RISK LEVEL
(Low, Moderate, or High)</td></tr>
<tr><td>ASSESSOR
Name:
Phone #:</td><td rowspan="2">RISK LEVEL IDENTIFIERS
(Use P(f) & C(f) Tables and R(f) Matrix)
R_f:
Probability of Occurrence (P_f):
Consequence of Occurrence (C_f):
Performance:
Schedule:
Cost:</td></tr>
<tr><td>ACTIVITY POC
Name:
Phone #:</td></tr>
<tr><td colspan="3">RISK DESCRIPTION & RECOMMENDATIONS:</td></tr>
<tr><td colspan="3">RISK LEVEL RATIONALE:</td></tr>
<tr><td colspan="2">ACTIVITY RESPONSE W/MITIGATION PLAN & SCHEDULE:</td><td>RISK OWNER/IPT
Name:
Phone #:
IPT:</td></tr>
</table>

DISCLAIMER: The Risk Assessment Team does not have the authority to direct the Contractor in any way nor alter the Contractor's contractual obligations. The Contractor shall take no action unless changes are issued in writing from the Contracting Officer. Any changes taken without official approval from the Contracting Officer shall be taken at the Contractor's own risk.

From (NSWC Corona, 2000)

Risk Identification Form

A Risk Identification Form (RIF), above, will be filled out for each risk identified during a risk assessment. Completed forms provide the Activity with the assessment results of each risk along with a description of the risk, risk level, and rationale for the risk level. The Activity, in turn, will have the opportunity to provide comments on each risk and a Plan of Action/Mitigation Strategies & Schedule.

The RIF will be completed in the following manner:

TRACKING NUMBER

This field contains a risk number prefix specific to the Functional Area Team that identified the risk and a sequential tracking number provided by the Risk Manager. The first set of digits should represent the Activity or Program being assessed. The second set of digits should represent the functional area or team that identified the risk. The last set of digits should be a sequential tracking number. A sample is provided below for a risk identified at Tank Factory #5 by the Production Team.

ACTIVITY--TEAM--NUMBER
(example: TF5--PROD--001)

RISK TITLE

Input a brief and descriptive title for the Risk. Be as specific as possible. A 3 to 5 word risk title is recommended.

PROCESS AREA

This block contains the most applicable Willoughby (Risk) Template and Template Category that the risk issue pertains to from the Risk Templates chart. In some cases, multiple templates and categories are acceptable. Example: Category: Production; Template: Defect Control.

FACILITY & PRODUCT/SUBASSEMBLY

Enter the Activity being evaluated and the hardware (and software) this risk write-up applies to in the "Product" field.

DATE IDENTIFIED

Enter the date this risk was identified.

DERIVED RISK LEVEL

This block contains the overall risk level for this risk based on the 5 X 5 Matrix Method and the "Risk Ruler." Rationale for this risk level must be documented in the Risk Level Rationale field using criteria and words from the "Risk Ruler."

ASSESSOR

This block contains the name, date, and phone number of the Assessor, the individual who identified this risk.

ACTIVITY POINT-OF-CONTACT (POC)

Enter the point-of-contact, the person responsible for this risk at the Activity.

REFERENCES

This block contains the documentation reviewed and personnel interviewed which aided in the discovery of the risk item.

RISK LEVEL IDENTIFIERS

For the identified risk enter the values for P(f), C(f), and the Derived Risk Level (Risk Factor-- R(f)) from the tables and matrices.

PROBABILITY OF OCCURRENCE RATING FACTOR P(f)

From the P(f) Table select a rating factor from 1 to 5 in increments of 1.0 using the criteria contained in the Table. The higher the number the higher the probability of occurrence.

CONSEQUENCE OF OCCURRENCE RATING FACTORS C(f)

From the C(f) Table select a rating factor for each impact parameter, i.e., Technical Performance, Cost, and Schedule. Use the criteria contained in the C(f) Table to arrive at rating factor selections. Rating factors are chosen from a range of 1 to 5 in increments of 1.0. Denote each rating factor selection in the applicable blocks of the risk identification form. Then choose the largest (maximum) C(f) rating out of the three chosen for each impact parameter. Cost, Schedule, and Performance are equally weighted. Use this largest (maximum) C(f) rating to obtain the Risk Factor.

RISK FACTOR R(f)

Use the selected values of P(f) and C(f) max above and find the intersection of P(f) and C(f) in the Derived Risk Level Matrix (cube). This is the Risk Factor R(f) rating also known as Derived Risk Level or Overall Risk Level. Annotate on the RIF in the Risk Level Identifiers Block and Derived Risk Level Block. Values may be modified as necessary by the qualitative risk criteria contained in the "Risk Ruler."

RISK DESCRIPTION & RECOMMENDATIONS

This block will provide a description of the risk and risk mitigation recommendations provided by the Assessor. Assessors will clearly address deficiencies observed using risk statements that start with a probable cause and iterate through causes and effects until an effect on cost, schedule, or performance is stated. Risk statements should be written in terms of "IF something happens" THEN "this is the impact on cost, schedule, and performance." IN ADDITION "this is how it is being done now and what is wrong about the approach." A list of recommendations should complete the risk statement. Cause and effect diagrams are an appropriate risk analysis and mitigation tool, which help to narrow the scope of the risk issue and to put it into consistent terms. It provides for consistency among Assessors and helps to determine risk mitigation actions. Additional paragraphs and continuation forms may be added as needed.

RISK LEVEL RATIONALE

Enter the rationale for assigning a particular risk level. This provides the Activity rationale for the risk write-up. The rationale statement(s) will address the Risk level and will provide rationale for why the risk exists. The Assessor will use words and phrases from the "Risk Ruler" criteria. Additional paragraphs and a continuation form may be added as needed.

ACTIVITY RESPONSE WITH MITIGATION PLAN & SCHEDULE

The block is filled out by the Activity being evaluated. It is the Activity's response to the identified risk. The Activity is responsible for identifying and documenting a risk mitigation plan with schedule for the identified risk. It must be documented or referenced on the RIF. If risk mitigation plans are large, they can be attached as a separate document, but must be at least referenced in this block of the RIF. Additional paragraphs and continuation forms may be added as needed.

RISK OWNER/INTEGRATED PRODUCT TEAM (IPT)

This block contains the name of the individual or IPT assigned risk mitigation responsibility.

DISCLAIMER

This item located at the bottom of the risk form in fine print is a reminder that Assessors cannot give contractual direction to Activities. All recommendations provided by Assessors are just that "recommendations" and if Activities act upon these recommendations they do so at their own risk. Only the Contracting Officer or equivalent can give contractual direction.

APPENDIX B. SAMPLE RISK CLASSIFICATION MATRICES

10 X 10 Matrix Method

	alogy.	moderately improve existing design.	minor requirement deficiencies.	items have been tested.	development approach and application.	manufacturing process
0.5	Existing technology and feasibility studies.	Major design change.	Some chance of minor requirement deficiencies.	Old design has been tested.	Readily adaptable s/w approach, conversion from similar application, expanded to new application.	Available Manufacturing Processes feasible by analogy
0.4	Proven technology and approach. Feasibility analysis complete.	Redesign, significant modifications.	Slight chance of minor requirement deficiencies.	Similar designs and technology have been tested.	Extensive modification and tailoring of existing approach.	Proven Manufacturing Processes but with no in house experience
0.3	Proven technology and approach, used some by design agent.	Existing proven components, recombined or minor mods in function.	Should meet all requirements with little margin.	Limited testing done on existing components.	Slightly modified approach, language conversion	Existing Manufacturing processes but newly established
0.2	Proven technology and approach with significant design agent experience.	Existing proven components, repackaged and/or minor usage variation.	Should meet all requirement, and exceed many.	Testing has been done on existing components.	Some modification of existing s/w approach.	Proven Manufacturing Processes used with limited experience
0.1	Proven technology and approach with significant design agent experience	Functional hardware. Mods in form only.	Will meet all requirements, exceeding many.	Thoroughly tested hardware.	Minor revision and checkout of existing s/w.	Proven Manufacturing Processes used with significant experience. (>2 years)
0.0	Off the shelf hdwr proven to operational environments.	Functional hardware.	Will exceed all requirements with margin.	Thoroughly tested and exceed reqmts.	Use of existing, checked out s/w.	NDI/ Off the Shelf Items

	Schedule Impact		Cost Impact		Technical	
RATING	SLIP PROBABILITY	AMOUNT	PROBABILITY	AMOUNT	ALTERNATIVES	Performance
.9	Certain, program threatening	>9 months	Certain, program threatening	> $900K DTC >9%	Cannot achieve.	Unacceptable.
.8	Extensive, Program threatening	>8 months	Extensive, Program threatening	> $800K DTC >8%	Redesign or alternate reqd to achieve	Inadequate.
.7	Probable program threat	>7 months	Probable program threat	> $700K DTC >7%	No adequate backup.	Significantly degraded
.6	Possible program threat	>6 months	Possible prog threat	DTC >6%	Inferior backup.	Degraded.
.5	Potential program threat	>5 months	Within uncertainty range.	> $500K DTC >5%	Several adequate alternatives.	Reduced.
.4	Serious subsystem slip with alternatives	>4 months	Well within acceptable range.	> $400K DTC >4%	Several adequate alternatives.	Slight reduction
.3	Subsystem slip requires workaround.	>3 months	Within budgeted range.	> $300K DTC >3%	Adequate alternatives exist	Minor reduction
.2	Minor subsystem slip.	>2 month	Minor.	> $200K DTC >2%	Many adequate alternatives.	Minor to none.
.1	Possible minor slip, noncritical path.	>1 month	Negligible.	> $100K DTC >1%	Many adequate alternatives.	No significant impact
0	No schedule impact.	None.	None.	None	Many adequate alternatives.	None.

From (Raytheon, 1999)

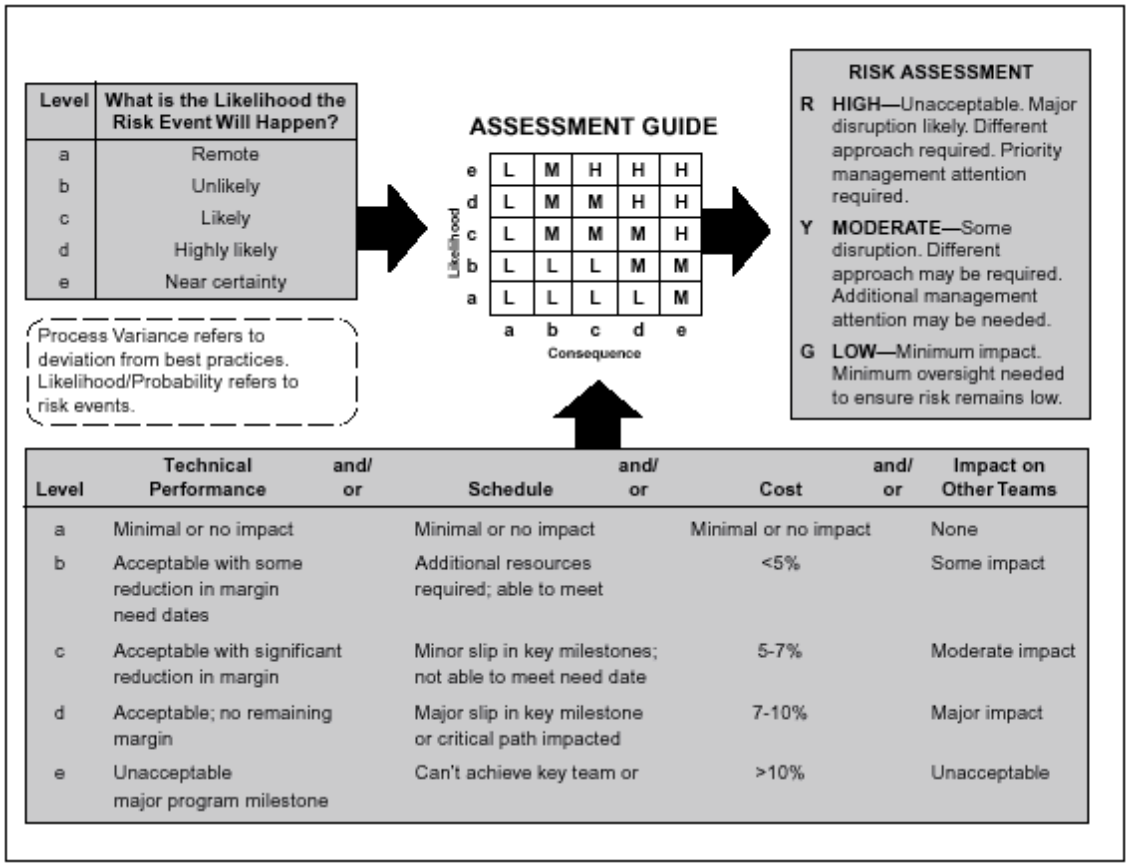
Probability of Occurrence (Pf)

Pf	Supportibility	Producibility	Requirements	Technology	Hardware	Software	Testing
0.9- 0.8	Support resource needs unknown; logistics characteristics (e.g.failure mode, repair process) unknown. Critical support resourc not available	No capability or technology to produce.	Unknown Rqmt or similar Rqmts haven't been implemented.	Maximum theoretical technology	Theoretical Design based on Advanced research.	New complex s/w; with untested applications or language.	Technology or approach not tested.
	Process Category: Near Certainty; Very Good Chance / Using An Unproven & Untried, Or No Process. There Are No Plans For Proving-In Process. There Is Not A Strategy or Current Strategy Will Not Resolve This Issue. Alternatives Will Be Required With Intense (Management) Attention						
0.7- 0.6	Surpport resource not fully defiend; *R & M significantlly below requirement	New manufacturing process required.	Undocumented Rqmt or major elements of rqmt beyond scope of previous systems.	Newer technology; Feasible by analogy; untested.	All new design.	Extensive s/w development; beyond experience base.	Technology Approach has limited testing.
	Process Category: Highly Likely; Good Chance. Using An Unproven But Tried Process. There May Be A Partial Plan And Schedule For Prove-In. Current Strategy Will Probably Fail To Resolve Issue. Alternative Plans Will Be Required.						
0.5- 0.4	Moderate resource shortfalls; *R & M below requirements.	Available Manuf processes feasible by analogy.	Unsure of Rqmt or expanded Rqmt from previously developed systems.	Existing technology and feasibility studies.	Major design change; significant modifications.	Extensive modification approach, conversion from similar application.	Old design or similar designs have been tested.
	Process Category: Likely to Occur; Even Shot / Using A Newly Proven (Untried) Process. Current Strategy May Or May Not Resolve This Issue. Alternative Plans May Be equired.						
0.3- 0.2	Minor resource shortfalls, or minor deficiencies in *R& M	Manufacturing processes have been used.	Requirement similar to previously developed systems.	Proven technology and approach; previously validated.	Existing proven components; recombined or minor mods in function.	Slightly modified approach, language conversion.	Previous exp with limited testing of new design.
	Process Category: Low Likelihood; Some Chance. Using A Proven But Unfamiliar Industry Practice. Current Strategy Should Resolve This Issue.						
0.1 - 0	Support resources dediend and available (people, data, equipment, spares) *R & M meets/exceeds requirements.	Proven Manufacturing processes used With significant Experience.	Requirements well within the scope of previously developed systems.	Proven technology and approach with significant design experience.	Functional h/w Mods in form only Minor usage variation.	Minor revision and checkout of existing software.	Thoroughly tested hardware.
	Process Category: Extremely Rare; Unlikely / Using A Proven & Familiar Industry Best Practice. Current Actions OK. Any Issues Easily And Quickly Resolved.						

Severity of Consequence (Cf)

Performance Impact			Schedule Impact		Total Cost of Ownership Impact	
C_f	Alternatives	Performance	Degree Of Impact	Mths		
1.0	No alternatives, program threat, need breakthrough	Key requirements not met	Major acquisition milestones, program threatened	>9	Certain program threat	Contractor Requests More Funding, or exceeds original program estimates >10%
0.9	Significant redesign required	Unacceptable unmet requirements	Major impact to customer plans	>8	Major impact to customer costs	
0.8	Redesign or alternate required	Usability degradation	Critical path events threatened	>7	Seriously affects other activities	
0.7	No adequate backup	Significant change from plan	Intermediate milestone revision with customer	>6	Revision with customer	Contractor overruns Management Reserve (MR), or exceeds original program estimate 7-10%
0.6	Inferior backup	Degraded	Significant program rescheduling	>5	Significant internal rebudgeting	
0.5	Possible alternative	Moderately reduced	Some effect on critical path	>4	Some internal rebudgeting required	Significant Reduction in Contractor's MR margin, or exceeds original program estimates 5-7%
0.4	Have adequate alternative	Slight reduction	Internal milestones slip with alternatives	>3	Changes within reserve	
0.3	A few adequate alternatives	Minor deficiency	Slip within IPT	>2	Minor within budget	Small Reduction in Contractor's MR margin, or exceeds original program estimates <5%
0.2	Many adequate alternatives	Acceptable changes	Minor IPT milestone changes	>1	Budget reallocated within current plan	
0.1	Many adequate alternatives	No significant impact	Possible minor slip; noncritical path	<1	Negligible increase	Minimal/No Impact
0.0	Many adequate alternatives	All requirements met	None	0	Negligible	

From (LPD 17, 2002)



From (DAU, 2002, p. B-17)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. RISK WRITE-UP EXAMPLE

Category: Production

Template: Manufacturing Plan

TRIMS Question #1: Are design engineers aware of manufacturing considerations during the development evolution?

Sample Risk Description & Recommendation: "**IF** the Contractor does not implement a concurrent engineering approach during development, **THEN** Manufacturing will have to redesign the hardware to make it producible which will significantly impact cost and schedule, with a potential impact on technical performance. **IN ADDITION**, design engineers are unaware of manufacturing needs and are not collocated with Manufacturing. The Contractor should implement a concurrent engineering philosophy and involve all key disciplines in the design & development process."

C_f (assess impact to cost, schedule, & performance assuming event has occurred):

Technical = 3: Moderate Reduction, Work-Arounds Available

Schedule = 3: Moderate Slip (May Affect Critical Path)

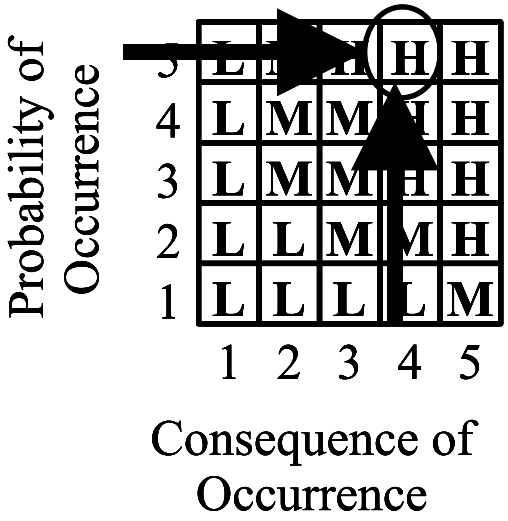
Cost = 4: Contractor/Activity Overruns Management Reserve (MR)

Take highest factor for $C_f = 4$

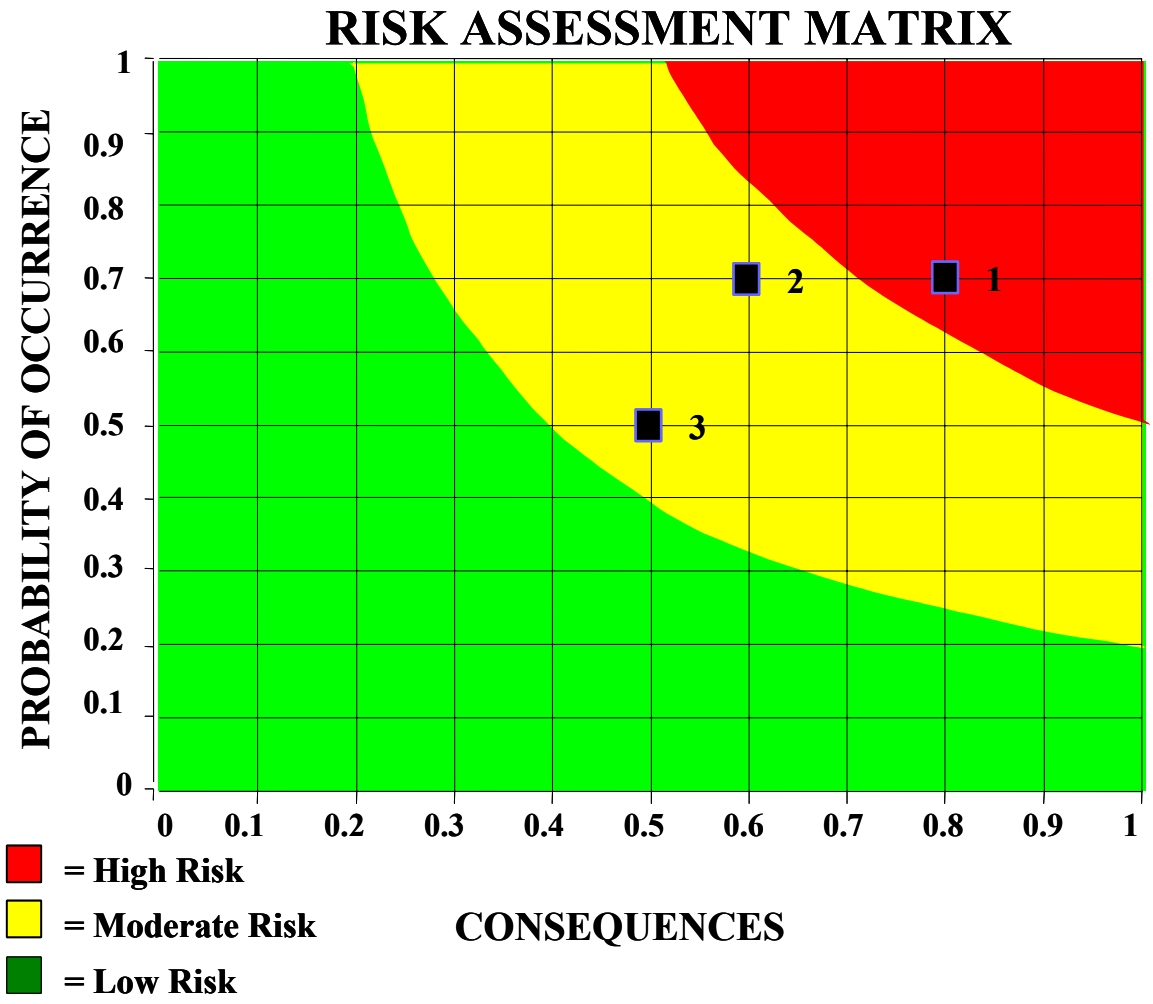
Risk Factor (R_f) = P_f X C_f = 5 X 4 = **High Risk**

Risk Level Rationale: Significant and substantial differences exist between standard and best practices. Contractor Management is not aware of the differences. There is no plan or schedule in place to implement a solution. Risk has a High probability of impacting cost, schedule, or performance. No slack time to implement a solution. An immediate high level of management attention is required.

H	High Risk
M	Moderate Risk
L	Low Risk

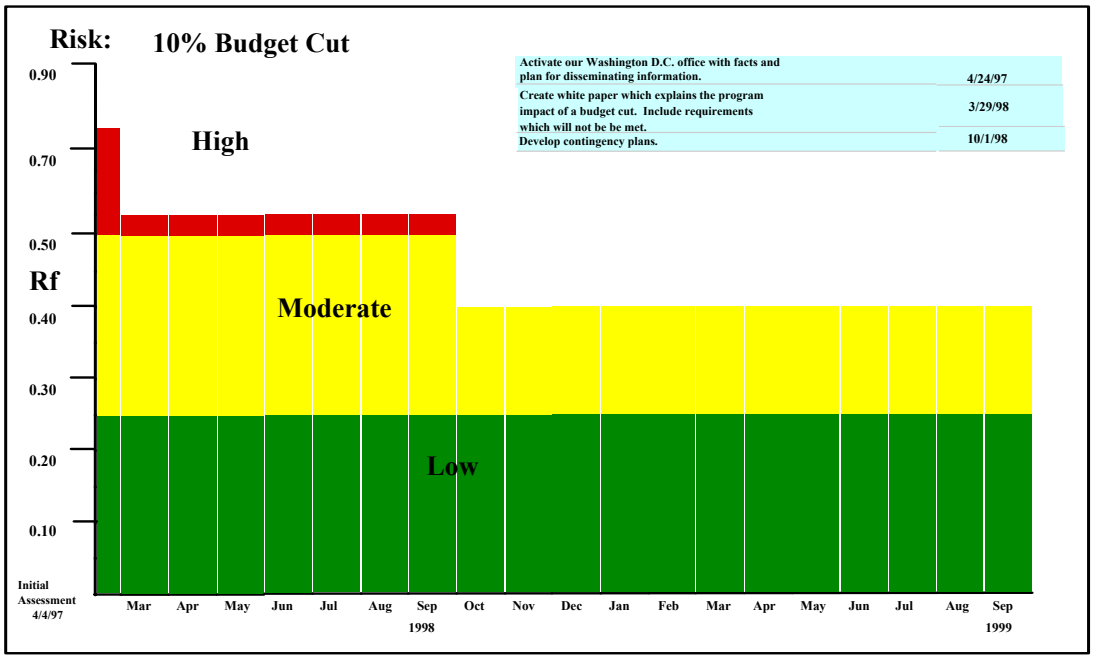


APPENDIX D. SAMPLE RISK REPORTING METHODS

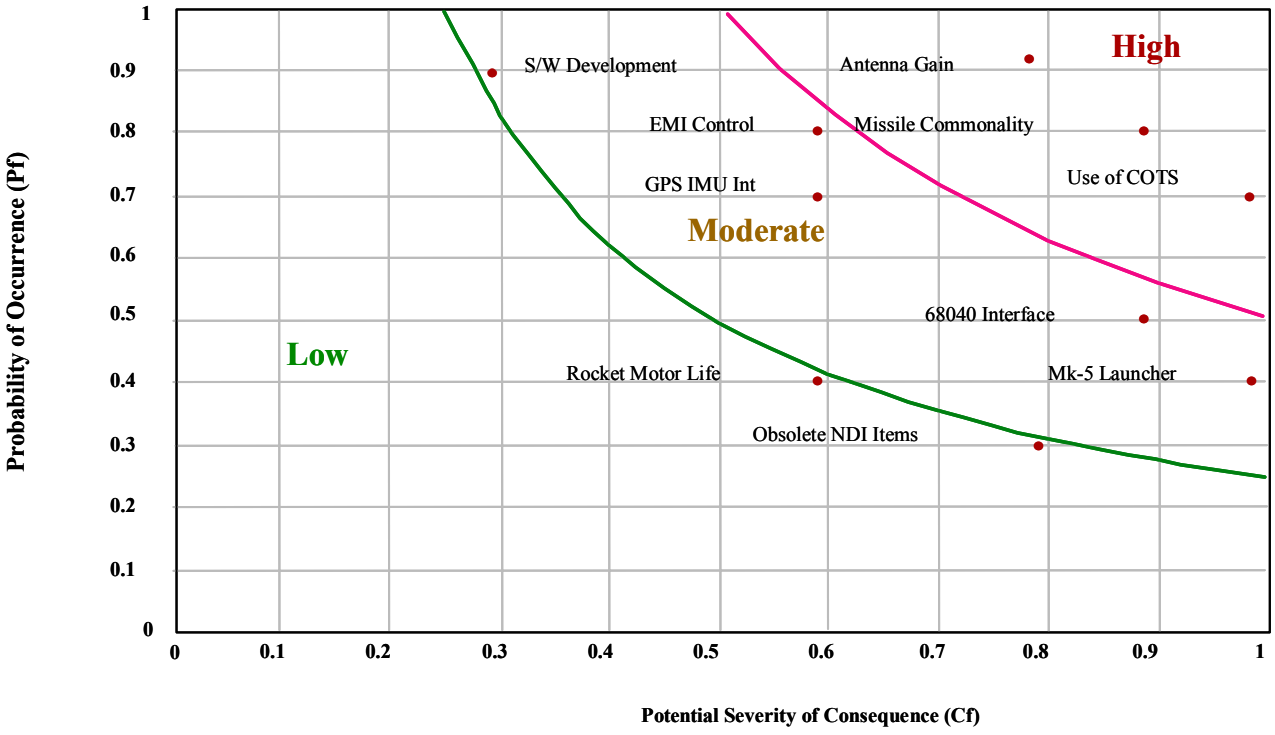


From (LPD 17, 2002)

A Waterfall Chart



The X-Y Chart



From (Raytheon, 1999)

APPENDIX E. TECHNICAL RISK MANAGEMENT SURVEY

Technical Risk Management Survey

Today's Date: _____

Name: _____
(Optional)

Phone: _____
(Optional)

DAWIA Career Field Category: _____ **Level:** _____
(Optional) (Optional)

Affiliation: Circle one

NAVSEA NAVAIR SPAWAR

Title/Job Function: _____

Years of Acquisition Experience: _____

Years of Risk Management Experience: _____

1. How important is Technical Risk Management to the success of an acquisition program?

   1 Extremely Important | 2 Very Important | 3 Important | 4 Somewhat Important | 5 Not Important

2. Do you consider Technical Risk Management a key component of program management?

   1 Strongly Agree | 2 Agree | 3 Neutral | 4 Disagree | 5 Strongly Disagree

3. How useful are <u>qualitative</u> Technical Risk Management methods, which are based on critical engineering processes, lessons learned, best practices, and check lists (e.g., Willoughby Templates, Methods & Metrics for Product Success, http://www.bmpcoe.org, etc.)?

   1 Extremely Useful | 2 Very Useful | 3 Useful | 4 Somewhat Useful | 5 Not Useful

   6 Don't Know

4. How useful are <u>quantitative</u> Technical Risk Management methods based on a Probabilistic Risk Assessment (PRA) methodology (e.g., fault trees, event trees, Monte Carlo simulations, etc.)?

   1 Extremely Useful | 2 Very Useful | 3 Useful | 4 Somewhat Useful | 5 Not Useful

   6 Don't Know

5. A Systems Engineering approach to acquisition program development better manages or minimizes technical risk.

   1 Strongly Agree | 2 Agree | 3 Neutral | 4 Disagree | 5 Strongly Disagree

6. Systematic, proactive identification and correction of faulty processes will significantly reduce the incidences of downstream acquisition problems.

   1 Strongly Agree | 2 Agree | 3 Neutral | 4 Disagree | 5 Strongly Disagree

7. Acquisition Reform increases the need for Technical Risk Management.

   1 Strongly Agree | 2 Agree | 3 Neutral | 4 Disagree | 5 Strongly Disagree

2

8. Technical Risk Management methods & techniques have changed drastically in the last 15 years.

1 Strongly Agree 2 Agree 3 Neutral 4 Disagree 5 Strongly Disagree

6 Don't Know

9. There is a risk awareness culture within my Program Management Office where program risks are identified and openly discussed.

1 Strongly Agree 2 Agree 3 Neutral 4 Disagree 5 Strongly Disagree

10. How important is a joint Program Management Office/Contractor Risk Management Program/Database for an acquisition program?

1 Extremely Important 2 Very Important 3 Important 4 Somewhat Important 5 Not Important

11. Risk mitigation plans should be loaded into the WBS/Project Schedule.

1 Strongly Agree 2 Agree 3 Neutral 4 Disagree 5 Strongly Disagree

12. Do you extend your Risk Management Program to include Software?

1 Yes 2 No (Go to #13) 3 Don't know (Go to #13)

a. What Software Risk Management methods do you use?

_____

13. Is your program using ASN (RD&A)'s NAVSO P-3686 "Top Eleven Ways to Manage Technical Risk" as guidance for your risk management program?

1 Yes 2 No 3 Don't know

14. Is your program using DoD 4245.7-M "Transition From Development To Production", NAVSO P-6071 "Best Practices" or ASN(RD&A) "Methods & Metrics for Product Success" (Jul 94) as guidance for your risk management program?

1 Yes 2 No 3 Don't know

15. Risk Management is perceived primarily as a source of workload rather than a part of the acquisition solution.

1 Strongly Agree 2 Agree 3 Neutral 4 Disagree 5 Strongly Disagree

16. How satisfied are you with the results of your Risk Management Program?

1 Very Satisfied 2 Satisfied 3 Neutral 4 Dissatisfied 5 Highly Dissatisfied

a. What are the key elements of your Risk Management Program?

_____
_____
_____

b. What successes have you achieved?

_____
_____
_____

c. What results were you hoping to achieve, where did you fall short?

_____
_____
_____

17. Have you received Risk Management training?

1 Yes 2 No (Go to #18) 3 Don't know (Go to #18)

Where did you acquire your training? (Institute & Course Title) _____

What methods were you taught? _____

18. Do you feel DoD, SECNAV, NAVSEA policy adequately address Risk Management requirements?

1 Strongly Agree 2 Agree 3 Neutral 4 Disagree 5 Strongly Disagree

19. What Risk Management policy and guidance documents are you familiar with?

_____

a. Which ones do you use on your Risk Management Program?

_____

20. What Risk Management policy and guidance documents are your contractors using?

_____
_____

21. Estimate the savings your Risk Management Program has provided (rough order of magnitude).

_____
_____
_____
_____
_____
_____

5

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. LINK TO THE SURVEY ON BMPCOE WEB SITE

BMP
Best Manufacturing Practices

Search Entire BMP Web Site
for GO

Award Winner
Innovations in American Government

Home | News & Events | Best Practice Surveys | Electronic Library | PMWS Software | The BMP Program | Links | FAQs

News & Events

BMP News

Seminars and Conferences

Search

Site Help

Site Map

Naval Post Graduate School Risk Management Survey

This survey is aimed at the acquisition professional, particularly program mangers and their staff, including support contractors and industry partners. The results will be used as a foundation for a Masters Thesis sponsored by Naval Post Graduate School, Office of the Assistant Secretary of the Navy (Research, Development and Acquisition) Acquisition and Business Management, Best Manufacturing Practices Center of Excellence (BMPCOE), and Naval Surface Warfare Center (NSWC) Corona Division. Survey responses will aid in the formulation of future Risk Management policy and guidance for the Navy. This survey should take no more than 10 minutes of your time. Thank-you. Michael Wheeler, Chief of Staff, NSWC Corona, (909) 273-5124, wheelerma@corona.navy.mil

http://www.zoomerang.com/survey.zgi?KXYLNJ93XB7Y4JPGVJ5G1M1G

Maintained by Webmaster
Best Manufacturing Practices Center of Excellence
Last Modified on : Wednesday, 24-Jul-02 10:27:46

APPENDIX G. TECHNICAL RISK MANAGEMENT SURVEY RESULTS

1.	How important is Technical Risk Management to the success of an acquisition program?	Number of Responses	Response Ratio
Extremely Important 1.		21	55%
Very Important 2.		14	37%
Important 3.		3	8%
Somewhat Important 4.		0	0%
Not Important 5.		0	0%
	Total	38	100%

2.	Do you consider Technical Risk Management a key component of program management?	Number of Responses	Response Ratio
Strongly Agree 1.		27	71%
Agree 2.		11	29%
Neutral 3.		0	0%
Disagree 4.		0	0%
Strongly Disagree 5.		0	0%
	Total	38	100%

3.	How useful are qualitative Technical Risk Management methods, which are based on critical engineering processes, lessons learned, best practices, and check lists (e.g., Willoughby Templates, Methods & Metrics for Product Success, http://www.bmpcoe.org, etc.)?	Number of Responses	Response Ratio
Extremely Useful 1.		7	18%
Very Useful 2.		19	50%
Useful 3.		8	21%
Somewhat Useful 4.		2	5%
Not Useful 5.		0	0%
Don't Know 6.		2	5%
	Total	38	100%

4.	How useful are quantitative Technical Risk Management methods based on a Probabilistic Risk Assessment (PRA) methodology (e.g., fault trees, event trees, Monte Carlo simulations, etc.)?	Number of Responses	Response Ratio
Extremely Useful 1.		5	13%
Very Useful 2.		10	26%
Useful 3.		12	32%
Somewhat Useful 4.		8	21%
Not Useful 5.		2	5%
Don't Know 6.		1	3%
	Total	38	100%

5.	A Systems Engineering approach to acquisition program development better manages or minimizes technical risk.	Number of Responses	Response Ratio
Strongly Agree 1.		23	61%
Agree 2.		13	34%
Neutral 3.		2	5%
Disagree 4.		0	0%
Strongly Disagree 5.		0	0%
	Total	38	100%

6.	Systematic, proactive identification and correction of faulty processes will significantly reduce the incidences of downstream acquisition problems.	Number of Responses	Response Ratio
Strongly Agree 1.		18	47%
Agree 2.		19	50%
Neutral 3.		1	3%
Disagree 4.		0	0%
Strongly Disagree 5.		0	0%
	Total	38	100%

7.	Acquisition Reform increases the need for Technical Risk Management.	Number of Responses	Response Ratio
Strongly Agree 1.		21	55%
Agree 2.		9	24%
Neutral 3.		3	8%
Disagree 4.		3	8%
Strongly Disagree 5.		2	5%
	Total	38	100%

8.	Technical Risk Management methods & techniques have changed drastically in the last 15 years.	Number of Responses	Response Ratio
Strongly Agree 1.		6	16%
Agree 2.		12	32%
Neutral 3.		7	18%
Disagree 4.		3	8%
Strongly Disagree 5.		0	0%
Don't Know 6.		10	26%
	Total	38	100%

9.	There is a risk awareness culture within my Program Management Office where program risks are identified and openly discussed.	Number of Responses	Response Ratio
Strongly Agree 1.		12	32%
Agree 2.		11	30%
Neutral 3.		8	22%
Disagree 4.		5	14%
Strongly Disagree 5.		1	3%
	Total	37	100%

10.	How important is a joint Program Management Office/Contractor Risk Management Program/ Database for an acquisition program?	Number of Responses	Response Ratio
Extremely Important 1.		12	32%
Very Important 2.		15	39%
Important 3.		9	24%
Somewhat Important 4.		1	3%
Not Important 5.		1	3%
	Total	38	100%

11.	Risk mitigation plans should be loaded into the WBS/Project Schedule.	Number of Responses	Response Ratio
Strongly Agree 1.		12	32%
Agree 2.		13	34%
Neutral 3.		8	21%
Disagree 4.		4	11%
Strongly Disagree 5.		1	3%
	Total	38	100%

12.	Do you extend your Risk Management Program to include Software?	Number of Responses	Response Ratio
Yes		24	69%
No		11	31%
	Total	35	100%

13	What Software Risk Management methods do you use?
#	Response
1	N/A
2	independent software engineering team, validation and verification, independent V&V, rational unified process (tm),
3	Metrics Reqmts trends -# -volatility -test ceverage/test completed S/W size trends -SLOC (new & Reused) Staffing trends -personnel-staff hours quality trends -STRs *status *age *priority -complexity *McCabe's *Mean and standard deviation Capacity trends -CRU Usage -Memory usage I/O Channel Usage Sked trends Automated tools to insure trceability and testability
4	We treat software risks like any other risk.
5	Risk Radar
6	N/A
7	We track a series of TPMs that were identified in the IBR process as well as added as additional needscame up. Those TPMs do not directly corellate to WBS tasks but they do follow the work flow so that consistent good performance on a TPM means low risk.
8	CMMI Results oriented
9	N/A
10	The most useful one right now is the one I created - checklists tied to systems engineering technical reviews (e.g. SRR, SFR, PDR, CDR, PRR, OTRR, etc)
11	Various
12	Software Fault Tree Analysis Review by Software Safety Technical Review Panel/ State Diagrams/Petri Nets
13	Not applicable
14	N/A
15	We use the SPMN Risk Radar. We Risk Officer assigned to all our programs at the program office, System Center and Contractor levels. Key risk areas are targets for process improvement. We have adopted software best practices to help woth software risk mitigation. We have implemented the SPMN 16 point plan on our programs which includes risk management. SPMN needs to be supported in the Navy as part of the risk management implementation process.
16	SW Managers Network & DOD PM's Guide to Software Acq Best Practices
17	The Risk Radar approach advocated by Software Program Mangaer's Network, modified by addition of "triggers" to alert when action needs to be taken.
18	Not applicable in my case. I am not managing a program.
19	have never used
20	Best Practices, Willoughby Templates, TRIMS

14.	Is your program using ASN (RD&A)'s NAVSO P-3686 "Top Eleven Ways to Manage Technical Risk" as guidance for your risk management program?	Number of Responses	Response Ratio
Yes 1.		13	36%
No 2.		13	36%
Don't Know 3.		10	28%
	Total	36	100%

15.	Is your program using DoD 4245.7-M, NAVSO P-6071 "Best Practices" or "Methods & Metrics for Product Success" as guidance for your risk management program?	Number of Responses	Response Ratio
Yes 1.		16	44%
No 2.		10	28%
Don't Know 3.		10	28%
	Total	36	100%

16.	Risk Management is perceived primarily as a source of workload rather than a part of the acquisition solution.	Number of Responses	Response Ratio
Strongly Agree 1.		2	5%
Agree 2.		10	26%
Neutral 3.		5	13%
Disagree 4.		17	45%
Strongly Disagree 5.		4	11%
	Total	38	100%

17.	How satisfied are you with the results of your Risk Management Program?	Number of Responses	Response Ratio
Very Satisfied 1.		2	6%
Satisfied 2.		14	39%
Neutral 3.		14	39%
Dissatisfied 4.		6	17%
Highly Dissatisfied 5.		0	0%
	Total	36	100%

18	What are the key elements of your Risk Management Program?
#	Response
1	not familiar enough with program office modes of operation
2	Identification of risks and mitigation efforts - tracked in documents but not tracked in time in a formal manner.
3	strong government encouragement of culture open to identifying risks; joint government contractor risk reviews, tehnical subject matter experts from government and university labs, TRIMs database and lessons learned, process rigor by asking the tailored, detailed TRIMS questions
4	Systems Engineering approachAll the players are at the table to include: -processess -contracts -logistics -engineering -test and evaluation -post IOC support -manufacturing -R&M -systems safety -quality -E3 -survivorability -S/W Key elements -risk identification -risk assessment -risk mitigation -risk mitigation plan execution (metrics to track, common reporting) -dispositioning the risk to an active single, data base ... to be used to understand the 'technical' health of the system -needs to be integral to the management of the program -open systems' safety and ORM into the PM's risk management process -on-going, iteraqtive process
5	Fostering an environment for teams to identify risks
6	Identification, mitigation planning, provides an overall understanding of program.
7	Our Risk Management Program is primarily an action tracking system for maintaining visibility of identified risks.
8	1. Identification of potential problems 2. Prioritization of risks 3. Implementing a risk tracking method 4. Involve the entire IPR in the process
9	We have a Program Office Risk Guide document that lays out some guidelines for monitoring Risk on a program. We incldue the contractor and TDA (CSS, Panama City) in our Risk identification and tracking method, called our Risk "Radar".
10	Product/Process Production Readiness Based Look at Potential Traps by asking the appropriate questions
11	We are just starting to implement a Risk Management Program in my program ofiice.
12	SSP practices Technical Program Management and has not "focused" on Risk Management as of yet.
13	Acquisition Risk Mgmt and System Operational Risk Management
14	Periodic Safety Reviews by WSESRB Risk Assessments for Flight Clearnaces Software/Hardware Weapon Fuzing Risk Reviews
15	Applying knowledgeable and empowered personnel to address myriad issues and challenges within programs ala applying the braintrust is the absolute best way to minimize risk. Government engineers are knowledgeable across multiple programs, far exceeding the contractors exposure to lessons learned. Each issue is unique and typically requires a tailored response - having great people applyiong their knowledge effectively through the use of deliverable CDRLs which require government approval makes sure the government gets the right product, on cost, on schedule and meeting performance.
16	My organization acts as risk management advocates for many program offices and employ most accepted risk management techniques.
17	Risk Radar Data Bases Risks are reviewed at all program reviews. We have a risk policy and risk officers We have trained all our personnel on risk management
18	Identifying the risks and weighting them appropriately.
19	Holding Joint Risk ID sessions with the contractor and all Govt support organizations. One full day of our quarterly program review is dedicated to identifying any new risks and development of mitigation and contingency plans
20	Risk Reviews
21	Incorporation of the results from SVRs and other reviews into the risk management system.
22	Proper visibility of the risks at the SEMT level.
23	Identification standard quantification management plans
24	The Risk Radar Database; fairly rigorous Risk Identification process; weekly review by APM with his team of risk status; bimonthly face-to-face review of risk status with upper management.
25	We help others conduct risk management using our TRIMS/PMWS tools
26	Performance, schedule, and cost
27	risk identification, analysis, mitigation, control, tracking, documentation
28	Communication of all issues to all Risk IPTs
29	Process & Product based Joint Contractor/Govt. Risk Database IPTs are empowered to identify risk Govt. and industry share the risk.

19	What successes have you achieved?
#	Response
1	can't answer
2	Clear identification of the highest risk areas and agreement from upper management on mitigation efforts to pursue.
3	-base lined 2 new starts, awaiting results -standardized risk reporting/assessment definitions -developed a NAVAIR S.E. guidebook - " " S.E. tech Risk Assessment Process Inst -developed a NAVAIR Risk Manage4ment inst
4	We've delivered major subsystems that meet and exceed customer expectations
5	Good tracking of overall program risk and the ability to understand funding priorities.
6	System has been effective in providing visibility of risks and tracking mitigation efforts.
7	1. Focus government attention on key contractual events which were key to meeting the program.(As a Sr. Contract & proposal Manager in Insustry.) 2. Trailoring the SOO and Contract Performance Planning prior to contract award.
8	We've had several succeses dealin with identifying Risk associated with new tasking that allowed us to get additional funds into our budget. Also, we identified several tactical Risks that we developed a propsoed solution for and then went ahead and tested the solution. In these cases 2 of the tactical risks (mine re-acquisition and depth localization) were succesfully mitigated, one (explosive shock) turned out to be unavoidable and is now being worked into our Op plan for the system. Most of our successes have been technical. There are too many to list in-total here but, for example, we succesfully reduced processor overhead (a risk identified early), Electro-static discharge through the towed body and EMI susceptibility.
9	Smooth transitions in Production Readiness for AEGIS Program Prime/Subcontractors
10	We are just starting to implement a Risk Management Program in my program ofiice. Some people have embraced the program, some have not.
11	N/A
12	Successes have varied from program-to-program. Successes are building since formulation and distribution of our risk checklists.
13	Elimation of potentially high risk designs from entering the Fleet.
14	Many early identifications of contractor risk, which has led to mitigation plans etc. F/A-18 E/F, V-22, JSOW, JDAM etc.
15	We measure success by a whether or not a program institutes a formal risk management program with insitutionalized processes for risk identification, analysis, reporting, and mitigation. Several have achieved this.
16	We have saved a number of our programs from failure. we are also being led to process improvements. We have a common lexicon accross all programs. We have linked performance appraisals to risk.
17	Heading off problems.
18	Schedules have been more realistically established that allow for our handling of schedule risks without negative impact to the program or the funding stream.
19	Avoided schedule and cost overruns
20	Risk management is performed at the IPT level.
21	Established balance of short ter.long term budget rqmts
22	In one case, we anticipated a loss of financial suuport for an up-coming experiment, and went out to alternaative sponsor who came through with the funds to allow the experiment to proceed on schedule.
23	We feel that the programs that have used TRIMS and/or the TRIMS methodology (process based RM) have benefitted; the more effectively they have used it, the greater have been the benefits.
24	Varies by program observed, and is dependant upon the method used. Programs using structured, measurable methods succeed. Programs not using risk assessment fail.
25	just getting a process documented. we also have identified our first risks, and the program manager is supportive of the process.
26	COTS Obsolescence risk mitigation, extending the life-cycle of COTS to match that of the program.
27	Successful milestone decisions

20	What results were you hoping to achieve, where did you fall short?
#	Response
1	can't answer
2	Identify system risks to allow decisions based on total system impact, versus typical situation where most powerful technical discipline 'gets its way'. We still are not able to eliminate skew towards undue weighting of risks to pet technical areas.
3	still strong risk identification adverse culture at Contractor
4	-on-going -instructions to be signed in several months
5	Subcontractors continue to be a problem area.
6	We do not predict or forestall risks. We only track them when they occur.
7	1. Fault free contract performance. Fault free program/contract performance
8	We were almost never suprised by a technical Risk. However, we fell short in connecting technical risks to schedule/cost risks. There are schedule/cost risks in every WBS element but we tracked technical risk separately and it wasn't alwasy celar how oen technical risk affected overall schedule.
9	N/A
10	N/A
11	Hoping to achieve order-of-magnitude increase in the understanding and ID of risk causal factors.
12	N/A
13	Biggest challenge is to translate technical risk assessment into terms the PM can understand.
14	Most programs we support that have risk management programs fall short by poorly identifying risks, failure to consider process related risks, and the screening or downplaying risks as they are reported up the management chain.
15	We have some program managers totall bought in and other hoping it will go away.
16	Systematic ease of risk management and identification.. missed some (not ID'd.)
17	I was hoping to have better buy-in from the other Govt agencies but I often find myself doing their risk identification.
18	Cannot control external risks
19	Without going into the expectations, one shortcoming is that we never seem to truely budget for risk mitigation/risk alternatives (i.e., no realistic "risk reserve"); also, there is always the danger of just going through the reviews without real scrutiny, lulling us into the perception that everything is fine because we are doing risk management, when we can miss the obvious. Maintaining the vigilance is a real challange.
20	Getting contractors to be willing to use TRIMS. You always have to fight the 'not invented here' attitude.
21	The results hoped for was actual itendification of risk, quantification of risk, and risk mitigation to an acceptable level. Acceptable level does not mean elimination of risk or even reducing all risks to low. It means the risk is manageable.
22	On other programs, most of the shortfalls is not communicating the risk from one program to the other when similar process/products are used (e.g. SM2BLOCK IVA AND SM-3, SM-2Block IV, III.
23	Hoping to quantify cost savings due to risk management program. Difficult to overcome the risk hiding culture. No one wants to hear bad news.

21.	Have you received Risk Management training?	Number of Responses	Response Ratio
Yes		31	82%
No		7	18%
	Total	38	100%

22	Where did you acquire your training? (Institute & Course Title)
#	Response
1	On-site training at NSWC Corona
2	Some training in conjunction with PD21 courses (NPS PD21 Software Engineering, NPS PD21 course with Ramesh Kolar)
3	DSMC APMC and PQM courses
4	OJT
5	I worked in the group at Hughes Aircraft that developed the corporate risk processes.
6	DSMC
7	DCMC - APMC HRO-CC(NAVSEA) - SoSovlving the Risk Equation (CSC) W. Edwards Deming/George Washington University - Quality, Productivity and Competitive Position
8	1. Rockwell-Collins Internal Course 2. Kepner-Tregoe course described in the book "Heads You Win! How the Best Companies Think -- and How You Cab Use Their Examples to Develop Critical Thinking Within Your Own Organization." Quinn Spitzer and Ron Evans, Published by Simon & Schuster.
9	I had an Enginering Risk class at NPS via the PD21 program but it wasn't very applicable We have a PMS 210 Risk Guide mentioned above which we are obliged to follow. Other than that I received no training.
10	NSWC, Corona
11	DSMC - PMC and EPMC
12	International Institute for Learning-Project Risk Management. Hewit Three day course. A two-day Risk Management Course developed by at NSWC Corona. A Technical Risk Management Course taught by ASN(RM&A)ADM Doug Paterson at Corona.
13	DSMC, and 31 years for OJT and exposure to the topic.
14	DAWIA
15	DAWIA/Defense Systems Management College Systems Engineering Development Program at China Lake in the early 1990's
16	PD21
17	APMC, DSMC
18	Provided internally by my organization
19	SPMN/ Mike Evans
20	On the ship under an Operational risk management presentation.
21	SPMN (Mike Evans)
22	SSC-SD SW Project Management Course DSMC PMT 302 SPAWAR Risk Mgmt, Metrics & Measures and Best Practices Overview
23	OTJ (On The Job)
24	Project Risk Management
25	DSMC APM course
26	Tim Lester,Atlantic Systems Guild, Inc., associated with the SPMN, came out to SPAWAR and gave us a three day course -- Software Risk management: the Nuts and Bolts
27	BMPCOE Brian Willoughby Gold Book training and other (including 'hands on').
28	Courses by ASN(RD&A) PI.
29	1) IIL, Project Risk Managment for NWAC 2)Various NSWC Risk Management courses on-site
30	NSWC Corona
31	NSWC Corona Dr. David Hulett (Cost & Schedule Risk Analysis)

23	What methods were you taught?
#	Response
1	5x5 matrix, 'Iron Triangle', others (don't remember...been too long)
2	Decision trees, formal risk management techniques
3	TRIMS and Best Practices
4	N/A
5	We use our own methods which align with accepted DoD practices.
6	SPC, TRIMS/Willoughby Templates
7	An action sequence that started with Situatiuon Appraisal followed by problem analysis and potential problem and Opportunity analysis.
8	N/A
9	Product/process based with use of TRIMs
10	DAU Handbook
11	5X5, using the Willoby Templates and TRIMS, Monte Carlo, 3X3, and 10X10
12	Mostly qualitative, which seems to work well.
13	Lots
14	Delphi Technique, Diagrammatic, Modified Churchman/Ackoff, Probability Density Function
15	PBA, Risk Tree Analysis
16	Monte Carlo, watchlists, etc.
17	Courses were primarily overviews. I do not have extensive training in specific risk management techniques.
18	Classroom nad Risk Management Symposiums with our contractors and System Centers. We have also trained our top management. we have run a risk ID session for SPAWAR with the SYSCOM Commander participating.
19	???? what methods are there?
20	Utilization of Risk Radar and the PM toolkit.
21	Qualitative, Quantitative, Cost and Schedule Analysis.
22	More than I use
23	Risk ID, Risk Analysis, Risk Reduction, Risk Tracking and Risk Control -- ultimately used Risk Radar produced by SPMN
24	TRIMS
25	Methods and Metrics for Product Success. TRIMS.
26	qualitative and a brief amount of quantitative
27	5x5 Matrix - Critical Path Templates.
28	Process based (Willoughby Templates and Best Practices) Cost and Schedule Risk Analysis using Monte Carlo Simulation

24.	Do you feel DoD, SECNAV, NAVSEA policy adequately address Risk Management requirements?	Number of Responses	Response Ratio
Strongly Agree 1.		0	0%
Agree 2.		15	43%
Neutral 3.		14	40%
Disagree 4.		6	17%
Strongly Disagree 5.		0	0%
	Total	35	100%

25	What Risk Management policy and guidance documents are you familiar with?
#	**Response**
1	I am familiar, although not well-versed with the "11-ways" and the BMP guides.
2	While I have encountered Risk Management in an academic setting, I do not see policy and guidance documents used explicitly at work.
3	DoD 4345.7M, NAVSO-P-6071, DoD 5000.2R, etc
4	DoD USAF Mil std 882
5	We use our own Risk Management Plan
6	NOne
7	NAVSO P-3686 "Top 11 Ways...) DoD 4245.7-M, NAVSO P-6071 "Best Practices" or "Methods & Metrics for Product Success"
8	DSMC Risk Management Guide
9	Dod 500.1 and DoD 5000.2R NAVSO P-3686 DoD 4245.7-M, "Transitioning from Dev. to Prod., Solving the Risk Equation" Defense Acq. Deskbook NAVSO P6071, "Best Practices to Avoid Suprises..."
10	TRIMs, BMP Database, Whilloghby Templates
11	DAU Handbook
12	Top Ten---Eleven ways to manage Risk. The BMP Best Practices, DOD 4275.M
13	The ones you reference above. We have also drafted two new NAVAIR instructions that address the topic - along with Handbook materials and checklists.
14	Various
15	DoD 5000-2R SECNAVINST 5000.2
16	DMSMS, sunset supplier program
17	Simply DOD 5000.2-R guidelines
18	DAU guidance
19	Willoughby Templates Top 11 ways to manage risk Methods and metrics for product success TRIMS DOD/DON 5000 Series
20	FAR, Acquisition Deskbook and our own policy in PMW 189.
21	No docs, I just use the concept
22	Truthfully I have never looked at the policies in detail. I did receive Risk Mgmt training as part of PMT 302
23	5000.2
24	Willoughby Templates, Top 11
25	"Top 11 ways..", "Methods and Metrix..", and NAVSO P-6071.
26	None by name
27	DoD 5000 ser DoD 4245.7M NAVSO P6071 NAVSO P3686
28	Methods and Metrics for Product Success. Willopughby Templates. 11 Ways to Manage Technical Risk.
29	DAU risk management guide, top 11 ways, best practices, willoughby templates, DoD 5000.2-R
30	ASN (RD&A)s NAVSO P-3686 "Top Eleven Ways to Manage Technical Risk"
31	Willoughby Templates NAVSO P-6071 Best Practices Methods and Metrics for Product Success NAVSO P-3686 Top Eleven Ways to Manage Technical Risk DAU/DSMC Risk Management Guide for DoD Acquisitions (5th edition, June 2002)

26	Which ones do you use on your Risk Management Program?
#	Response
1	can't answer
2	I do not believe any particulay policies or guidance documents are formally followed when program managers in my field consider risk.
3	all
4	-DoD good referenc - Wills Templates -Mil STD 882 -
5	NOne
6	TRIMS BMP
7	N/A
8	Our Risk Guide is a flow-down of the documents above. I basically use it, though I ahve a copy of P-3638
9	All of the above
10	DAU Handbook
11	Do not yet have a "Risk Management Program"
12	Primarily the checklists tied to specific SE technical reviews.
13	Various
14	DoD 5000.2-R, NAVAIR Risk Assessment, WSESRB Risk Assessment procedures
15	DMSMS, sunset supplier program
16	Typically implement what we can during spec development activities.
17	All listed above
18	Our own PMW policy
19	More policies and programs. Why should there be so many? Why not just some intuitive software to help guide the concept.
20	5000.2
21	Same as #25
22	See response to items 14 and 15.
23	Don't know -- we use the Risk Radar. I don't know what the source policy document is for it
24	Teach and Promote 4245 and 6071 as embodied and expanded in TRIMS
25	Varies from all to none.
26	all of the above
27	ASN (RD&A)'s NAVSO P-3686 "Top Eleven Ways to Manage Technical Risk"
28	NAVSO P-3686 Top Eleven Ways Willoughby Templates NAVSO P-6071 Best Practices Methods and Metrics TRIMS

27	What Risk Management policy and guidance documents are your contractors using?
#	Response
1	can't answer
2	I am not sure.
3	same, and their own Risk Register
4	n/a
5	N/A
6	None
7	Company proprietary Risk Mgmnt tool. See #18 above.
8	N/A
9	Good question. I have noidea. They do have a copy of our guide though and the cotnractually have to follwo the DoD 5000 documents.
10	Whilloughby templates
11	N/A
12	Various.
13	Various
14	Unknown, but most have a Risk Management Board under Acquisition Reform Initatives.
15	DMSMS, sunset supplier program
16	not sure
17	Those listed above
18	They have their own policy
19	Don't know
20	Contractor's
21	Same as #25
22	See response to items 14 and 15.
23	N/A
24	Our contractors are using the same techniques we use
25	My most recent experiences is none.
26	all of the above
27	NA
28	unknown

28	Estimate the savings your Risk Management Program has provided (rough order of magnitude).
#	Response
1	can't answer
2	Unable to say.
3	n/a
4	NA
5	N/A
6	This is hard. I'd say $2 - #3M/year for technical risks. It could be much, much higher for the tactical risks (say and Order of Magnitude).
7	N/A
8	N/A
9	Impossible to calculate savings, but I would guess on the order of 10-25% of total acquisition cost.
10	??
11	$100K-$500K (ROM)
12	savings are hard to pin down - the success of the program is the only real metric that gets high visibility to me.
13	I have no insight to this information
14	That is too hard. Its cost avoidance and grief avoidance.
15	UNK
16	$400-500K
17	Impossible to quantify
18	Savings a Risk Management Program provides cannot be measured.
19	too difficult to quantify
20	0
21	Unk.
22	don't know at this time
23	NA
24	Cannot quantify

29	Name (optional), Phone (optional), Title/ Position, DAWIA Career Field Category & Level, Years of Acquisition Experience, Years of Risk Management Experience.
#	Response
1	Meg Stout (202) 781-2416 DAWIA PM II, SPRDE II 5 years PM, 18 years SPRDE 5 years associated with some risk management efforts
2	Denise Bolton Transition to Production Engineer Standard Missile Program Office PEO-TSC 15 yrs acq experience, 5 yrs risk mgmt experience
3	Mike Persson/301.342.7118/Systems Engineering Processess& Policy, AIR 4.1G 10 years experince in the acquistion arena
4	Russ Stahlak 858-522-4467 Program Manager at Raytheon Electronic Systems
5	John Thornton 619-524-7033 Program Manager PM LEvel III 15 Year acquisition experience 6 Year risk exp
6	General Engineer/Production Manager DAWIA Program Management Level III Acquisition/Risk Mgmt Experience - 25+ years
7	R. Marshall Engelbeck, Lecturer,GSB&PP, NPS. Acquisition Management, 20yrs of experience, All 20 of them but I didn't realize it until the last 4 or 5.
8	- Jon Etxegoien - 202-781-1622 - Not yet DAWIA Certified - 4 years of Acqusition experience, 2 in a program office - 2 years Risk Management experience
9	Rod MacKinnon, 619-524-7653 Program Manager, SPAWAR PMW 182 DAWIA PM lvl III certified, 20 yrs Acq Exp, 8 yrs risk management.
10	Steve Nelson, 909-823-6861, Engineer in QA 14 Government Programs at NSWC Corona, PQM Level III certified, 18 years and two of risk management.
11	Bob Skalamera 301-757-6640 APEO(SE) AIR-1.0 Programs S3, PM3 ~24 years of acquisition experience ~12 years risk management experience
12	Ken Chirkis, DSN 437-0600, Supervisory Safety Engineer (DP-3/GS-803-13), DAWIA Code= "S" Systems Engineering, 15 Years of Experience in Acquisition, 22 Years of Experience in Risk Management
13	Graham Lester Navigation Sales Manager RD Instruments
14	Dale Moore Director, Aerospace Materials Division NAVAIR Sys R&E & PM lvl III 20 year experience
15	Keith Snider (831) 656-3621 Associate Prof PM level III 11 years Acq Exp
16	Manager, SPRDE level III, 18 years, 1 year as a manager of an organization heavily involved in risk management, 17 years working closely with the subject but somewhat on the periphery.
17	Frank Doherty, Deputy PM, PMW 189, SPAWAR, over 25 years of acquisition experience wih 10 years of Risk Management experience.
18	CDR, Division Hd. in PMW. Still awaiting level 2 PM courses. PM level 1 SPRDE level 2 6 years What qualifies as risk management? I used ORM 15 years ago as a DIVOFF.
19	APM for Cooperative Development Program (US & UK). PM Career field, Level 3, 6 years Acq Experience, 8 years mgmt
20	Assistant Program Manager PM Level 3 15 Years Acq & Risk Mgmt Experience
21	Dr. M. Ripp PQM II ~15 years experience

22	Robert Dworshak PQM 7 6
23	Robert Ernst (301) 342-2203 DAWIA - Systems Engineering 18 yrs acq experience Risk - 6 yrs experience
24	Head of Technolgy and Andvanced Development Division in SPAWAR PMW 189 Program offfice for Naval Electronic Combat Surveillance Systems; PM III; 17 years Acq exper; 4 years Risk Mgmt Exper (formally)
25	Charlie Minter, Technical Risk Manager BMPCOE
26	Mike McCune Deputy Executive Director NSWC Corona Division (909) 273-5001 SPRDE 20 Years Acquisition 3 Risk Management
27	mechanical engineer, DAWIA-SPRDE level 3, 12 years acquisition experience, 3 years risk management experience
28	Raymond Tadros, 909-273-4209, Mechanical Engineer, SYS Engineering (SPRDE), 5yrs, 3yrs.
29	Michael Wheeler, (909) 273-5124, Chief of Staff NSWC Corona, Level III PM, Level III Systems Engineering, 16 years, 12 years

30. Affiliation		Number of Responses	Response Ratio
NAVSEA		16	42%
NAVAIR		8	21%
SPAWAR		9	24%
VIEW Other, Please Specify		10	26%

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

American Graduate University and Procurement Associates. (1998). *Risk Analysis and Management*.

Assistant Secretary of the Navy, Research, Development & Acquisition, Acquisition & Business Management (ASN(RD&A)ABM). (1997). *Risk Management Survey of Department of the Navy Programs*.

Best Manufacturing Practices Center Of Excellence (BMPCOE). (2000). *TRIMS - Technical Risk Identification and Mitigation System*. [Tutorial]. Minter, C.: Author.

Best Manufacturing Practices (BMP) Program Manager's Workstation (PMWS). (n.d.). Retrieved August 11, 2002, from http://www.bmpcoe.org/pmws/index.html

Center for Defense Information (CDI). (n.d.). *Military Industrial Complex*. Retrieved July 26, 2002, from http://www.cdi.org/issues/usmi/complex/

Chronicle of the Falklands / Malvinas History and War of 1982. (n.d.). Retrieved July 28, 2002, from http://www.yendor.com/vanished/falklands-war.html

Clark, J. J., & Johnson, T. D. (2002). *A Primer on Acquisition Logistics*. Retrieved July 21, 2002, from http://www.almc.army.mil/alog/issues/MayJun02/MS757.htm

CMU/SEI-95-MM-02, *People Capability Maturity Model*. (1995). Retrieved August 15, 2002, from http://www.sei.cmu.edu/publications/documents/95.reports/95.mm.002.html

CMU/SEI-96-TR-023, ESC-TR-96-023, *Cleanroom Software Engineering Implementation of the Capability Maturity Model for Software*. (1996). Retrieved August 15, 2002, from http://www.sei.cmu.edu/publications/documents/96.reports/96.tr.023.html

CMU/SEI-97-HB-002, *Software Acquisition Risk Management Key Process Area (KPA)—A Guidebook Version 1.0*. (1997). Retrieved August 15, 2002, from http://www.sei.cmu.edu/publications/documents/97.reports/97hb002/97hb002abstract.html

CNN Interactive. (n.d.). *Military-Industrial Complex Speech*. Retrieved July 26, 2002, from http://asia.cnn.com/SPECIALS/cold.war/episodes/12/documents/eisenhower.speech/

Dalton, J. H. (1998). *A Worthy Class*. Remarks to DoN Acquisition Hall of Fame Acquisition Pioneer Awards Ceremony, May 13, 1998, Pentagon, Virginia. Retrieved August 5, 2002, from http://www.chinfo.navy.mil/navpalib/people/secnav/dalton/speeches/acq0513.txt

Defense Acquisition University (DAU). (2002). *Risk Management Guide for DoD Acquisition* (5th ed.). Retrieved August 18, 2002, from http://www.dau.mil/pubs/gdbks/risk_management.asp

DefenseLink. (n.d.). *Acquisition Reform*. Retrieved July 21, 2002, from http://www.defenselink.mil/execsec/adr95/acq_.html

Defense Spending may be the Mother of all Invention. (2002). Retrieved July 24, 2002, from http://www.redherring.com/investor/2002/0114/718.html

Defense Systems Management College (DSMC). (n.d.). *What Led to Acquisition Reform.* Retrieved July 21, 2002, from http://www.dsmc.dsm.mil/jdam/contents/what_led.htm

Defense Systems Management College (DSMC). (n.d.). *Federal Acquisition Streamlining Act (FASA).* Retrieved July 21, 2002, from http://www.dsmc.dsm.mil/jdam/contents/fasa.htm

Defense Systems Management College (DSMC). (n.d.). *What is Acquisition Reform?* Retrieved July 21, 2002, from http://www.dsmc.dsm.mil/jdam/contents/whatis.html

Defense Systems Management College (DSMC). (n.d.). *Cultural Change.* Retrieved July 21, 2002, from http://www.dsmc.dsm.mil/jdam/contents/cultural.htm

DoD 3020.36-P*, Master Mobilization Plan*. (1988). Retrieved July 23, 2002, from http://www.dtic.mil/whs/directives/corres/html/302036p.htm

DoD 4245.7-M, T*ransition from Development to Production…Solving the Risk Equation*. (1985). Assistant Secretary of Defense, Acquisition and Logistics.

Federation of American Scientists (FAS) Military Analysis Network. (n.d.). *MK 92 Fire Control System (FCS)*. Retrieved July 28, 2002, from http://www.fas.org/man/dod-101/sys/ship/weaps/mk-92-fcs.htm

Federation of American Scientists (FAS) Military Analysis Network. (n.d.). *MK 15 Phalanx Close-In Weapons System (CIWS).* Retrieved July 28, 2002, from http://www.fas.org/man/dod-101/sys/ship/weaps/mk-15.htm

Higgs, R., (1995). *World War II and the Military-Industrial-Congressional Complex*. Retrieved July 26, 2002, from http://www.independent.org/tii/news/950501Higgs.html

Hulett, D.T., (2001). *Key Characteristics of a Mature Risk Management Process*. Retrieved August 15, 2002, from http://www.risksig.com/articles/euro2001/hulett.pdf

Hulett, D. T., & Campbell, B., (2002). *Integrated Cost / Schedule Risk Analysis*. Retrieved August 15, 2002, from http://www.risksig.com/articles/index.htm#ARTICLES FROM PMI EUROPE 2002

Goldwater-Nichols and Acquisition Reform Legislation. (n.d.). Retrieved July 29, 2002, from http://www.rand.org/publications/MR/MR1438/MR1438.ch2.pdf

IPPD Definitions and Key Tenets. (1995). Retrieved July 21, 2002, from http://www.npd-solutions.com/ippdtenets.html

John Fitzgerald Kennedy (JFK) Library. (n.d.). *Special Message to the Congress on Urgent National Needs, President John F. Kennedy*. Retrieved July 17, 2002, from http://www.cs.umb.edu/jfklibrary/j052561.htm

LPD 17. (2002). *Risk Management*. From a briefing given to the LPD-17 community.

Methods & Metrics for Product Success. (1994). Office of the Assistant Secretary of the Navy, Research, Development & Acquisition (OASN(RD&A))

Mobilization—the U.S. Army in WW II the 50th Anniversary. (n.d.). Retrieved July 14, 2002, from http://www.army.mil/cmh-pg/documents/mobpam.htm

Montgomery, D. C. (2001). *Introduction to Statistical Quality Control* (4th ed.). New York: John Wiley & Sons, Inc.

NASA. (2002). *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners* (Ver. 1.1). Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC

NASA Historical Reference Collection. (n.d.). *Chapter 5 Operations Apollo 204 Fire*. Retrieved July 17, 2002, from http://www.hq.nasa.gov/office/pao/History/Apollo204/biblio.html

NASA History in Brief. (n.d.). Retrieved July 17, 2002, from http://history.nasa.gov/brief.html

National Conference of Standards Laboratories (NCSL). (n.d.). *Papyrus Story*. Retrieved July 14, 2002, from http://www.ncsli.org/misc/cubit.cfm

National Defense University Library (NDUL). (n.d.). *Goldwater Nichols Department of Defense Reorganization Act of 1986*. Retrieved July 29, 2002, from http://www.ndu.edu/library/goldnich/goldnich.html

Naval Surface Warfare Center (NSWC) Corona. (2000). *Technical Risk Management*. From a technical risk management class presented by Michael Wheeler.

NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*. (1998). Office of the Assistant Secretary of the Navy, Research, Development & Acquisition (OASN(RD&A)) Acquisition and Business Management (ABM).

NAVSO P-6071, *Best Practices – How to Avoid Surprises in the World's Most Complicated Technical Process*. (1986). Department of the Navy.

Osgood, J. (1996). *The Goldwater Nichols Act – Managing the Defense Department*. Retrieved July 29, 2002, from http://pw1.netcom.com/~jrosgood/w16.htm

Pate-Cornell, M. E., Fischbeck, P. S., (1994). "Risk Management for the Tiles of the Space Shuttle," *Interfaces*, 24, 64-86.

PEOTSCINST 3058.1, *Risk Management*. (2000). Program Executive Office Theater Surface Combatants

Perry, W. J., (1994). Memorandum Subj: *Specifications & Standards - A New Way of Doing Business*. Retrieved July 22, 2002, from http://www.dsp.dla.mil/policy/perry.html

Powell, J. E., "The Case For COTS," *COTS Journal*, May 2002, pp. 65-68.

Preparation for Flight, the Accident, and Investigation. (1967). Retrieved July 28, 2002, from http://history.nasa.gov/search?NS-search-page=document&NS-rel-doc-name=/office/pao/History/SP-4009/v4p1g.htm&NS-query=Willoughby&NS-search-type=NS-boolean-query&NS-collection=History&NS-docs-found=1&NS-doc-number=1

Pressman, R. S. (2001). *Software Engineering – A Practitioner's Approach* (5th ed.). New York: McGraw-Hill.

Raytheon Missile Systems Company. (1999). *Risk Management – Decisions Often Involve Risk…Manage the Risk!* From a presentation by Rana Lavu.

Reig, R. W. (2000). "Baselining Acquisition Reform," *Acquisition Reform Quarterly—Winter 2000*. Retrieved July 22, 2002 from http://www.dsmc.dsm.mil/pubs/arq/2000arq/reig.pdf

Rosenberg, L. H., Hyatt, L. E. (1997). *Software Quality Metrics for Object-Oriented Environments*. Retrieved August 7, 2002, from http://www.stsc.hill.af.mil/CrossTalk/1997/apr/quality.asp

Sandia National Laboratories. (n.d.). *Risk Assessment and Risk Management*. Retrieved August 13, 2002, from http://www.sandia.gov/E&E/ram.html

Schach, S. R. (1999). *Classical and Object-Oriented Software Engineering* (4th ed.). New York: WCB/McGraw-Hill.

Schaeffer, M. D. (1997). "IPPD—One Year After," *PM: Special Issue*, January – February 1997. Retrieved July 21, 2002, from http://www.dau.mil/pubs/pm/pmpdf97/schaeffe.pdf

Sheehan, K. (2001). *E-mail Survey Response Rates: A Review*. Retrieved August 24, 2002, from http://www.ascusc.org/jcmc/vol6/issue2/sheehan.html

Software Program Manager's Network (SPMN). (n.d.). *Risk Radar Version 2.02*. Retrieved August 27, 2002, from http://www.spmn.com/rsktrkr.html

Stamatelatos, M., (2000). *Probabilistic Risk Assessment: What is It and Why is It Worth Performing It?* Retrieved August 13, 2002, from http://www.hq.nasa.gov/office/codeq/qnews/pra.pdf

SURTASS Risk Management Training Student Guide. (2002). Naval Surface Warfare Center, Corona Division

The Likert scale. (n.d.). Retrieved August 24, 2002, from http://www.cultsock.ndirect.co.uk/MUHome/cshtml/index.html

The Railroad Gauge. (n.d.). Retrieved July 14, 2002, from http://www.design.caltech.edu/Misc/rail_gauge.html

What is Monte Carlo Simulation? (n.d.). Retrieved August 15, 2002, from http://www.decisioneering.com/monte-carlo-simulation.html

Why Do We Need IPTs? (n.d.). Retrieved July 21, 2002, from http://osdipt.dynsys.com/Chapter_1/1b.html

Willis Willoughby Inducted into Navy Acquisition Hall of Fame. (1998). Retrieved August 5, 2002, from http://pma265.navair.navy.mil/reports/1998/980513.html

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Coyle, P. E., "Evolutionary Acquisition – Seven Ways to Know If You Are Placing Your Program at Unnecessary Risk," *PM*, November-December 2000.

Defense Acquisition Deskbook. Defense Acquisition University (DAU). From http://web2.deskbook.osd.mil/default.asp?

Department of Defense Directive Number 5000.1, Change 1, January 4, 2001. *The Defense Acquisition System*. USD(AT&L).

Department of Defense Instruction Number 5000.2, April 5, 2002. *Operation of the Defense Acquisition System*. USD(AT&L).

Department of Defense Regulation Number 5000.2-R, April 5, 2002. *Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs*. USD(AT&L), ASN(C3I), and DOT&E

Forsberg, K., Mooz, H., Cotterman, H. (2000). *Visualizing Project Management* (2nd ed.). New York: John Wiley & Sons, Inc.

Gemmer, A., Risk Management: Moving Beyond Process," *Computer*, May 1997.

Shaffer, G., "Controlling COTS Risks – A Practical and Systematic Approach," *COTS Journal*, February 2002.

Umansky, E., "Studs and Duds," *The Washington Monthly*, December 2001.

United Stated General Accounting Office Report (GAO-01-244). (January 2001). *Major Management Challenges and Program Risks – Department of Defense*.

United Stated General Accounting Office Report (GAO-02-701). (July 2002). *BEST PRACTICES – Capturing Design and Manufacturing Knowledge Early Improves Acquisition Outcomes*.

United Stated General Accounting Office Report (GAO-98-56). (February 1998). *BEST PRACTICES – Successful Application to Weapon Acquisitions Requires Changes in DoD's Environment*.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Mr. Bill McAninch
   OASN(RD&A)ABM
   Arlington, Virginia

4. Mr. Charlie Minter
   BMP Center of Excellence
   College Park, Maryland

5. Mrs. Mary Lacey
   Naval Surface Warfare Center
   Washington Navy Yard, District of Columbia

6. Dr. A. Wayne Meeks
   Naval Sea Systems Command (SEA 53)
   Washington Navy Yard, District of Columbia

7. Mr. Mike McCune
   Naval Surface Warfare Center, Corona Division
   Corona, California

8. Mr. Ramesh Kolar
   Naval Postgraduate School
   Monterey, California

9. Mr. Wally Owen
   Naval Postgraduate School
   Monterey, California

10. CAPT Mike Persson
    Naval Air Systems Command (AIR 4.1G)
    Patuxent River, Maryland

11. Mr. Frank Doherty
    Space and Naval Warfare Systems Command (PMW 189)
    San Diego, California

12. Mr. Douglas Patterson
DynCorp
Daytona Beach, Florida

13. Mr. Thomas Higbee
Space and Naval Warfare Systems Command (05A)
San Diego, California

14. Mr. John Thornton
Space and Naval Warfare Systems Command (PMW 183)
San Diego, California

15. Mr. Michael Wheeler
Naval Surface Warfare Center, Corona Division
Corona, California